iGuard

IP/Network Camera
User's Manual
300 Series

LIMITED HARDWARE WARRANTY

Warranty Coverage

Micon Technology Inc. ("MICON") warrants to the original purchaser that the **iGuard IP camera product line** enclosed with this limited hardware warranty will in respect of the hardware be free from defects in design, workmanship and materials under normal use for a period of one (1) year from the date of the original purchase ("Warranty Period").

The original purchaser shall without undue delay notify MICON of any defect which appears according to MICON's RMA Procedure, failure to which shall mean that the purchaser surrenders its right to have the defect remedied. A valid form of a bill of sale or receipt from an authorized retailer/distributor with the date of the original purchase must be presented to obtain warranty service. If a valid claim is received within the Warranty Period, the sole remedy of the original purchaser and MICON's sole and exclusive liability shall be limited to, at MICON's sole discretion, either repair of the hardware defect using new or refurbished replacement parts, or replacement of the product. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. When a product or part is exchanged the replacement hardware becomes the property of the original purchaser and all hardware or part thereof that is replaced shall become the property of MICON.

Exclusions and Limitations

This warranty does not apply (a) to faulty and improper installation, maintenance, service, repair and/or alteration in any way that is not contemplated in the documentation for the product or carried out with MICON's consent in writing, operational adjustments covered in the operating manual for the product or normal maintenance, (b) to cosmetic damages, (c) if the product is modified or tampered with, (d) if the product is damaged by acts of God, misuse, abuse, negligence, accident, normal wear and tear and deterioration, improper environmental conditions (including, but not limited to, electrical surges, water damage and heat exposure) or lack of responsible care, (e) if the product has had the model or serial number altered, defaced or removed, (f) to consumables (such as batteries) (g) to products that have been purchased "as is" and MICON, the seller or the liquidator expressly disclaim their warranty obligation pertaining to the product, (h) to any non-MICON hardware product or any software (irrespective of packaged or sold with an MICON hardware product) and MICON products purchased from an unauthorized distributor/reseller,(i) to damage that occurs in shipment or (j) to damages by any other causes not related to defective design, workmanship and/or materials.

NOTE:

- If the product is to be used outdoors or in dusty, humid, or other hostile environments, it must be suitably protected.
- Further, camera products specifically, must be protected, whether in use or not, from exposure to direct sunlight or halogen light – which may damage the camera image sensor. This applies to both indoor and outdoor use of the cameras.
- For camera products supplied without a lens, extreme care should be used when mounting a lens on these products. Damage to the product due to incorrectly mounted lenses will invalidate this limited hardware warranty.
- Failure to comply with any of the aforementioned requirements will invalidate this Limited Hardware Warranty.

THE WARRANTY AND REMEDIES PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CERTAIN JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES. IF LAWS UNDER SUCH JURISDICTIONS APPLY, THEN ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED TO THE WARRANTY PERIOD IDENTIFIED ABOVE. UNLESS PROVIDED HEREIN, ANY STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. EXCEPT AS PROVIDED IN THIS WRITTEN WARRANTY AND TO THE EXTENT PERMITTED BY LAW, NEITHER MICON NOR ANY AFFILIATES SHALL BE LIABLE FOR ANY LOSS, (INCLUDING LOSS OF DATA AND INFORMATION), INCONVENIENCE, OR DAMAGE, INCLUDING, BUT NOT LIMITED TO, DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, RESULTING FROM THE USE OR INABILITY TO USE THE MICON PRODUCT, WHETHER RESULTING FROM BREACH OF WARRANTY OR ANY OTHER LEGAL THEORY. NOTWITHSTANDING THE FOREGOING, MICON' TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS WARRANTY SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES HAVE BEEN AN ESSENTIAL CONDITION IN SETTING THE PRODUCT PRICE.

DISCLAIMERS

SOFTWARES INCLUDED WITH ALL IGUARD IP CAMERAS AND MICON DDNS SERVICE ARE PROVIDED BY MICON “AS IS” AND MICON , ITS DISTRIBUTORS AND SUPPLIERS EXPRESSLY DISCLAIM ALL EXPRESS, IMPLIED, AND STATUTORY WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING:

(i) MICON MAKES NO WARRANTY THAT THE SOFTWARE AND SERVICE WILL BE EFFECTIVE, RELIABLE OR SECURE;

(ii) MICON MAKES NO REPRESENTATIONS OR WARRANTIES WHATSOVER ABOUT ANY THIRD PARTY CONTENT, PRODUCTS OR SERVICE THAT MAY BE OFFERED OR PURCHASED WITH ITS PRODUCTS;

(iii) MICON MAKES NO REPRESENTATION OR WARRANTY THAT YOUR PREMISES OR PERSONS OR PROPERTY ON YOUR PREMISES WILL BE SAFE OR SECURE; AND

(iv) MICON DOES NOT WARRANT THAT THE SOFTWARE AND DDNS SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE, THAT DEFECTS WILL BE CORRECTED, OR THAT THE SERVICE OR THE SERVER THAT MAKES IT AVAILABLE ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.

LIMITATION OF LIABILITY

TO THE FULLEST EXTENT ALLOWED BY LAW, MICON AND ITS DISTRIBUTORS AND SUPPLIERS WILL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF USE, COST OF COVER OR OTHER, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE SERVICE, THE SOFTWARE OR THE SITE, INCLUDING, WITHOUT LIMITATION, ANY LIABILITY FOR:

(i) DAMAGES TO PREMISES, PERSONS OR PROPERTY ARISING OUT OF OR RELATING TO THE USE OF THE SOFTWARE OR INABILITY TO USE THE SOFTWARE,

(ii) DAMAGES ARISING OUT OF SERVICE UNAVAILABILITY, AND

(iii) DAMAGES CAUSED BY THIRD PARTY PRODUCTS OR SERVICES,

THE FOREGOING LIMITATIONS OF LIABILITY WILL APPLY WHETHER IN AN ACTION FOR BREACH OF CONTRACT, NEGLIGENCE, OTHER TORT, OR ANY OTHER THEORY, EVEN IF AN AUTHORIZED REPRESENTATIVE OF MICON HAS BEEN ADVISED OR SHOULD HAVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES.

OUR LIABILITY, AND THE LIABILITY OF OUR AFFILIATES, AND SUPPLIERS, TO YOU OR ANY THIRD PARTIES IN ANY CIRCUMSTANCE IS LIMITED TO THE AMOUNT PAID FOR THE PRODUCT OR SERVICE. THE FOREGOING DISCLAIMERS, WAIVERS AND LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OF CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

CONTENTS

Chapter 1 Introduction **1**

1.1 Features 1

1.2 Application 1

1.3 iGuard IP Camera Line 2

Chapter 2 Hardware Installation **4**

Chapter 3 Software Installation **7**

Chapter 4: iGuard Utility **8**

4.1 Setup Wizard 9

4.2 Launch iGuard 12

4.3 IP Configuration 13

4.4 Upgrade Firmware 15

Chapter 5 iGuard Web Manager **17**

5.1 Introduction 17

5.2 iGuard Web Manager Interface 17

5.2.1.1 Video Streaming 18

5.2.2 Information 21

5.2.2.1 System Status 21

5.2.2.2 Current Connections 21

5.2.2.3 Event Log 22

5.2.3 Basic Settings 23

5.2.3.1 Camera Settings 23

5.2.3.2 Network 24

5.2.3.3 Wireless Setting 29

5.2.3.4 Account Settings 30

5.2.4 Advanced Settings 32

5.2.4.1 Event Notification 32

5.2.4.2 Motion Detection 36

5.2.4.3 Scheduled Recording 39

5.2.4.4 E-mail / FTP 40

5.2.4.5 System Settings 43

5. 2.4.6 About 45

5.2.5 USB Disk 46

Chapter 6: iGuardView **48**

6.1 Adding Cameras ____ 49
6.2 Camera Setting ____ 52
6.3 Motion Detection Setting ____ 53
6.4 Email Notification Setting ____ 55
6.5 SNMP Setting ____ 56
6.6 Schedule Recording ____ 57
6.7 Camera Monitor ____ 57
6.8 MuiltiView ____ 61
6.9 System ____ 61
6.10 Help ____ 62
Chapter 7: iGuard Mobile ____ 63
Appendix A: Network Configuration /Router Programming ____ 66
Appendix B: IP Address, Subnet and Gateway ____ 86
Appendix C: Glossary ____ 88
Appendix D: Q&A ____ 89

Chapter 1 Introduction

1.1 Features

iGuard is a series of affordable, versatile and flexible IP based remote monitoring solutions for small business, retail store, and residential applications. iGuard features a built-in web server (iGuard IP-101S and 301S module) with a range of USB cameras to choose from, eliminating the need to have a computer to stream video images to the internet. Each system can simultaneously support any two combinations of digital cameras be it embedded or standalone, regular or infrared, fixed or pan-tilt. With its upgraded web-video-server, the new 300 series iGuard IP cameras allows the user to stream video to the internet through a wired or wireless network and record images directly on to an attached USB drive or to the hard-drive on a remote PC. The included iGuardView PC based client software allows the user to monitor and record multiple cameras on one PC.

Features:

- Built-in Web-Video-Server
- 10/100Mbps Fast Ethernet Network Access
- WiFi Ready (through optional USB wireless dongle)
- Support Any Java-Enabled Web Browser
- Built-in LCD display (on selected models)
- Built-in RS232 Port
- 32-Bit ARM9 Processor
- 4MB Flash Memory
- 16MB Dynamic Memory
- Support Up to 30 Remote Viewers for each camera
- Allow Up to 8 User Accounts and Passwords
- 5.3VDC 1A Maximum
- Operating Temperature: 0°C ~ 60°C
- Operating Humidity: 10% ~ 90%
- Network Protocol: HTTP, TCP/IP, UDP, SMTP, PPPoE, Dynamic DNS, DNS Client, SNTP, BOOTP, DHCP, FTP, SNMP
- Support All USB PC Camera with VIMICRO ZC0301^{+} DSP processor
- Resolution: 640 x 480, 320 x 240, 160 x 120.
- Frame Rate: Up to 30 @ 320 x 240
- Motion JPEG streaming video, MPEG-4 recording
- 2 USB Ports for USB Cameras (One available for embedded cameras)
- USB 1.1 & 2.0 compliant
- USB DVR Function (with optional USB drive)
- Support Pan/Tilt and Infrared USB PC Camera

1.2 Application

The most important function of iGuard is for remote surveillance. Once iGuard is installed, the user can monitor any of the connected iGuard cameras via any web

browser. The user can monitor and control these cameras simply by entering the IP address of the iGuard from anywhere in the world as long as there is an Internet connection. For instance, the user can be in the United States but he or she can monitor the production facility in China, and if he or she likes, also check on the branch office in Singapore at the same time.

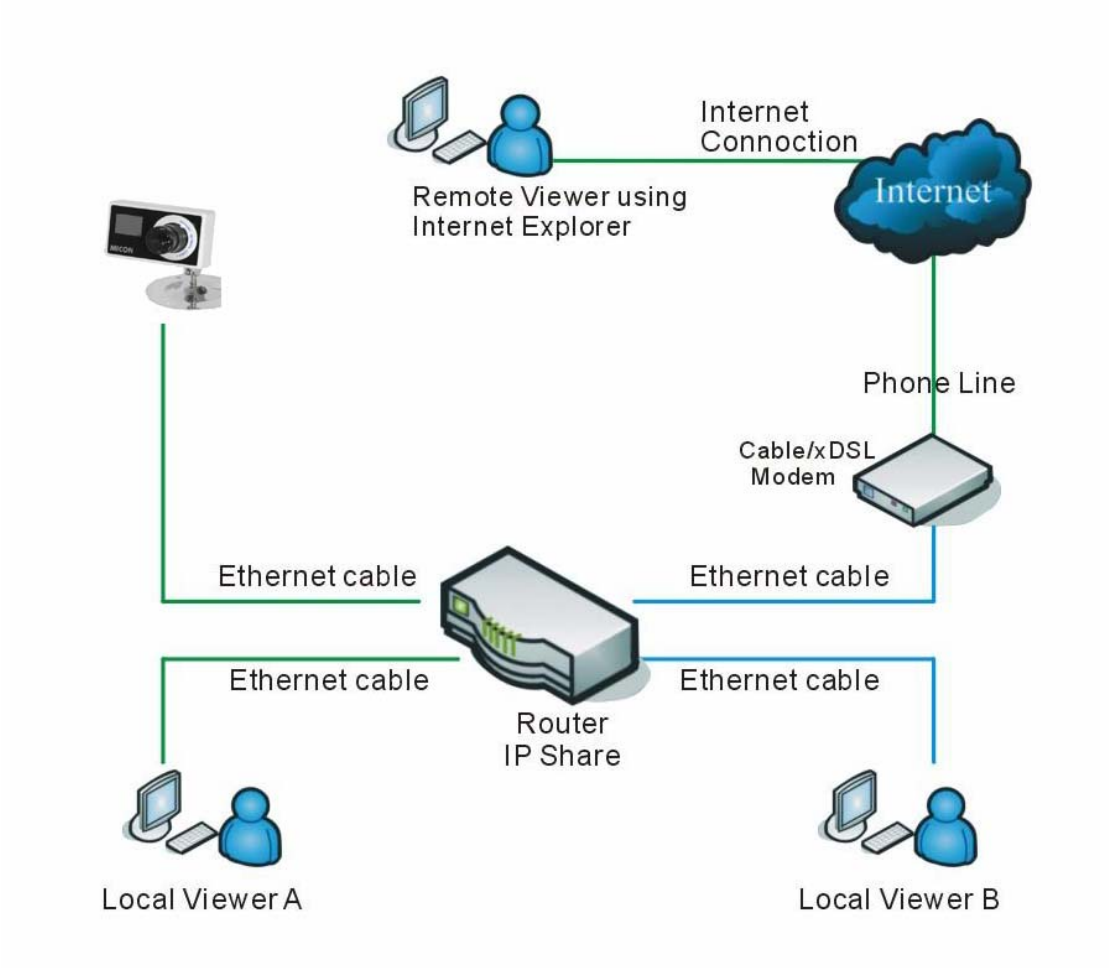


Fig.1. iGuard Network Diagram

1.3 iGuard IP Camera Line

Following is a list iGuard IP/Network cameras that is avail be for purchase. All cameras within the series share the same network and imaging technology, whether embedded or stand alone. The 300 series adds the wireless and USB DVR capability as well as a RS232 expansion port to the 200 series. Please check www.iguard.com for latest list of iGuard offerings, following is a list of current models.

1.3.1 iGuard 200 series IP Cameras

 IP-280E	 IP-103K	 IP-220E
 IP-250E	 IP-101K	 IP-210E

1.3.2 iGuard 300 Series IP cameras

 IP-380E	 P-310E	 IP-320E

1.3.3 iCam Add-on cameras

 iCAM-04	 iCam-01	 iCam-03

Chapter 2 Hardware Installation

Installation of iGuard hardware is fairly straightforward. The procedures are pretty much the same for all iGuard IP cameras. Please refer to the "Quick Installation Guide" in the package for your specific model. As an example, shown below are the steps to set up iGuard IP-310E IP camera.

Make sure a network connection and AC power are readily available at the location where the camera will be installed. We suggest you program the camera first before you physically installed the camera. It is assumed you have basic knowledge about networking and you have access (login) to the router on the network.

A. Package Content.



Your iGuard package should contain the following items;

1. iGuard IP/Network Camera,
2. 10-100 Ethernet Cable
3. iGuard Utility CD/Software
4. Quick Installation Guide.
5. 5.3V DC Adapter
6. Mounting Hardware (for selected models only)

Contact your dealer immediately if any of these items are missing.

B. Camera Installation



First familiarize yourself with the physical layout of the camera. For IP-310E there are 4 jacks as shown on the right picture

- Power-In (5.3V DC)
- Ethernet (RJ-45)
- USB Expansion
- IO (RS232)



1. **Prepare for the Installation**
   You need to provide power and LAN access (if you choose to install the camera via its lan port) near the location where the camera will be installed. Do not cut and extend the AC adapter. Use a proper extension cord if necessary instead.

2. **Mount the Camera**
   Mount the bracket first (You may wish to use the included anchors to secure the bracket). Attach the camera to the bracket's universal panning head.



3. **Adjust the Camera Angle**
   Loosen the knob on the bracket's universal panning head and adjust the camera to the desirable angle. Hand-tighten the knob.

C. Expansion Installation (Optional)

iGuard 300 series IP cameras have a built-in USB expansion port, to which a second USB camera, a wireless dongle, or a USB storage device can be attached.



1. **USB Add-on Camera**
   A large selection of USB cameras can be used as a second camera. Once attached the second camera icon will lid and will be designated as camera B.



2. **Wireless Dongle**
   You can attach a USB WiFi dongle to connect the camera to wireless network. A wireless icon will lid if a compatible WiFi dongle is attached. For wireless network setup please refer to section 5.2.3.3 in Chapter 5

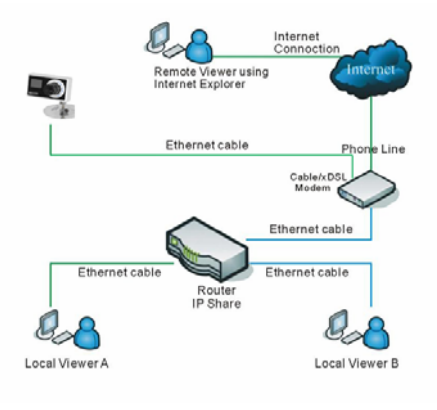


3. **External Storage**
   You can attach a USB storage device including flash drives and iPods to the camera to store video and images locally on the camera. A disk icon will lid if a compatible USB drive is attached. For USB DVR recording please see Section 5.2.4.2 and 5.2.4.2 in Chapter 5.



4. **USB Hub**
   If you wish to use two or more of the above options simultaneously, you can attach a compatible USB Hub (we recommend using self-power hubs)

D. Internet Connection



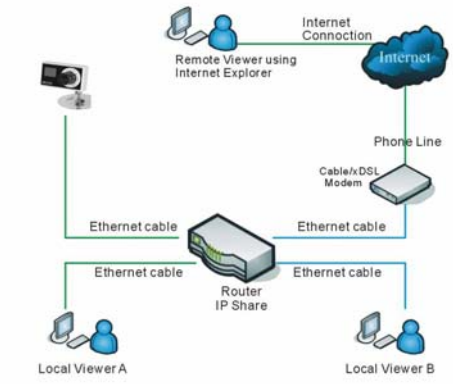
1. **Cable/DSL Modem Connection**
   You can connect the IP-310E to a cable/DSL modem directly if you have dedicated internet connection.

2. **Router/Switch Connection**
   If you use a router to share internet connection then your camera has to be connected to the router which in turn is connected to the cable/DSL modem.

3. **IP Configuration**
   By default IP-310E will obtain an IP address assigned by a DHCP-enabled router, and display that IP on the LCD screen. You can skip directly to ***Chapter 5*** to configure and monitor the camera via its web manager

E. Power On

Connect DC power output into iGuard DC-in socket, and plug the DC power adapter into the wall socket.

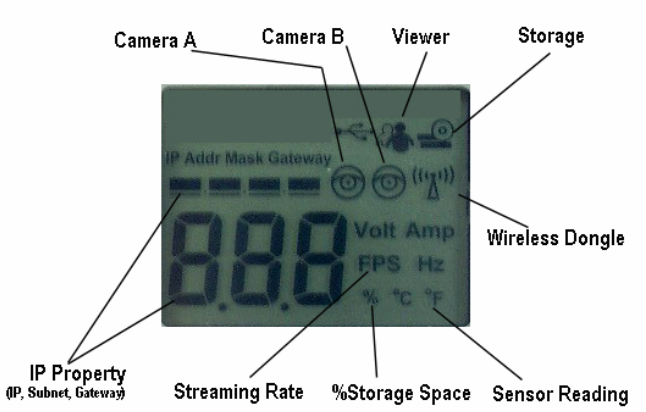




Warning:
Do not cut and extend the DC cord, use a proper extension cable if necessary!

F. LCD Display*

The built-in LCD screen on the iGuard (iGuard IP-310E, 210E, 250E, and 103K), will display the IP address assigned by a DHCP server on the network, as well as other host of information. You can skip directly to the iGuard web manger (Chapter 5) by launching the Internet explorer and enter the IP address on the LCD.



Note:

* For iGuard models without the built-in LCD, the easiest way to set up the camera is through iGuardUtility which will be discussed in next chapter.

Chapter 3 Software Installation

On the utility CD there is a collection of two programs: iGuard Utility and iGuardview, collectively called as iGuardware You can use the iGuard Utility to quickly setup any iGuard cameras on the network, whether it has a built-in LCD or not. You can use iGuardview to monitor and record multiple cameras.

Insert the software CD (or download the latest version from www.iguard.com) and click on setup.exe if autorun does not start.

An installation menu will be displayed on you screen:



Fig.2. iGuardware Installation

- **iGuard Utility** - This is a program that helps the user perform quick installation. It will detect the current configuration and take the user through the necessary network setup.
- **iGuardView** - This is a windows based program designed to allow user to control a large number of iGuard cameras located either in a LAN or on a WAN.
- **Read User's Manual** - Click to read iGuard's User Manual. You will need Adobe Acrobat Reader v5.0 or higher.
- **Adobe Acrobat Reader v5.0** - This will install Acrobat Reader v5.0 on your local hard drive.
- **Sun Java / ActiveX** - Install Sun Java for viewing the video image by Java, or install the OCX for viewing by ActiveX

Chapter 4: iGuard Utility

iGuard Utility is a setup program for iGuard cameras, whether the camera has a built-in LCD or not. You can launch iGuard Utility by clicking on “Start/Programs/ iGuard/iGuard Utility/”

The main menu is shown below. The selection menu is located on the left. The Serial Number, current Firmware and IP Address of every iGuard connected to the LAN will be displayed in the table to the right. All buttons except “about” and “Refresh” will be disabled if there are no iGuard camera detected on the network.



Fig.3. iGuard Utility Main Menu

If the password on your unit is not enabled and you are on the same LAN (same subnet) then you can launch the web manager to configure the iGuard camera simply by double click on the “Launch iGuard” button or the highlighted iGuard displayed in the window. Everything discussed in this chapter can be repeated in Chap.5

4.1 Setup Wizard

"Setup Wizard" will take you through the basic configurations step by step.

1. Click to highlight the iGuard that you want to configure.

2. Click on "Setup Wizard". Enter the administer login ID and Password if promoted



Fig.4 iGuard Setup Wizard

Note: *By default the administer login ID and Password is not defined, therefore the login screen will not be displayed*

3. The camera setup window.



Fig.5 iGuard Setup Wizard

Choose the appropriate light source (Indoor 60 Hz, Indoor 50 Hz or Outdoor) to prevent flickering or whiteout on the video streaming. Enter a name for the camera in the “Location” box to easily identify it.

4. Click “Next >” to configure the IP property.



Fig.6 iGuard Network Setup

“Obtain an IP address by DHCP”

Choose this if you are installing the iGuard on a network with a DHCP server. Make sure to set the IP lease time to “Permanent” in your router so that the IP address assigned to the camera will not change.

“Use the following IP Address”

Enter an appropriate IP Address, Subnet Mask and Gateway for iGuard if have a static IP to assign to the iGuard.

“Obtain an IP address by Bootp”

Allow iGuard to obtain an IP address using Bootp protocol.

5. Click “Next >” to proceed to xDSL/Cable modem setup.



Fig7 iGuard a/DSL Setup

If iGuard is the only device on your DSL network and your ISP supports PPPoE, Select ***"Enable PPPoE connection"*** and enter your account and password details as provided by your internet service provider ("ISP").

Note: *You may need to subscribe to a DDNS service If you have a DLS account with a dynamic IP.*

Otherwise, leave it at the default ***"Disable PPPoE connection"***

6. Click "Next >" to change your administrator account and password for the iGuard ***web manager***. (chapter 5)

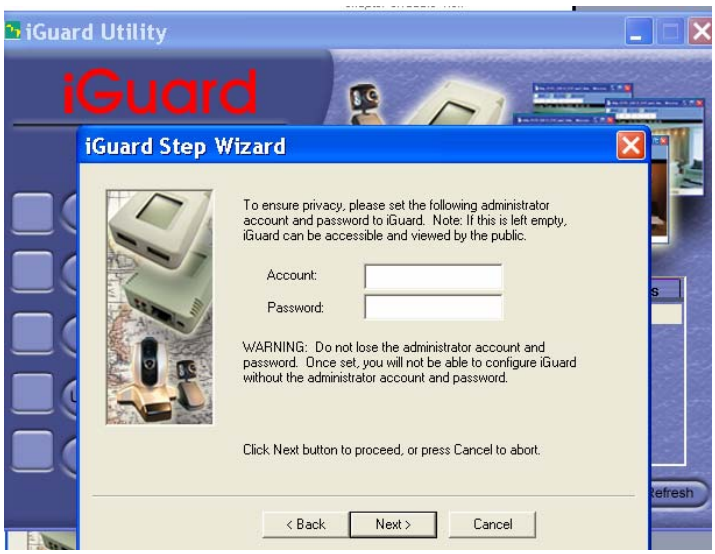


Fig.8 iGuard a/DSL Account Setup

By default the administrator account is defined. It is recommended to define at this stage. Be advised all iGuard Passwords are case-sensitive.

WARNING:
Do not lose the administrator account and password. Once set, you will not be able to configure iGuard via its web manager without the administrator account and password. To reset the iGuard account password, you will have to refresh the firmware or use the master password to retrieve it.

7. Click “Next >” to upload these configuration to iGuard.

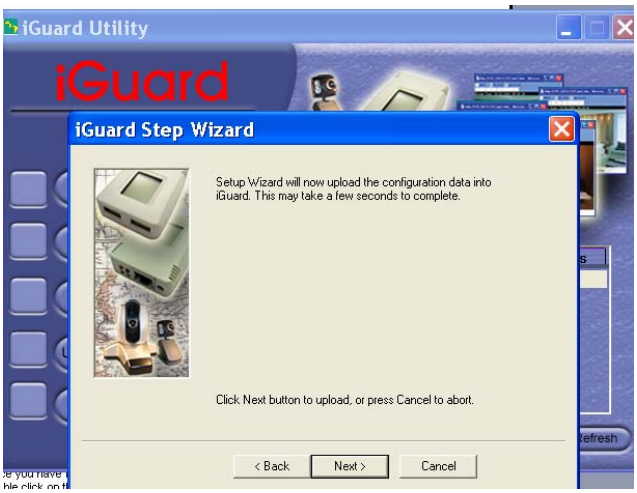


Fig.9 iGuard Account Setup

8. Click “Finish” to restart iGuard with the new configurations.

4.2 Launch iGuard

Once you have finished with the above Setup Wizard, either click “Launch iGuard” or double click on the iGuard listed on the table, You will be bring to the iGuard Web Manager (Chapter.5).



Fig.10 Launching iGuard

Type in the account name and password entered earlier (if you did not configure one, just press ENTER or click on the “Apply” button)

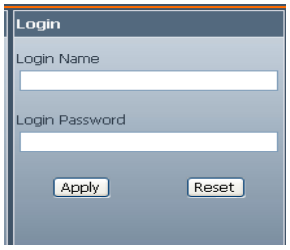


Fig.11 iGuard Web Login

Please refer to Chapter 5 for more details.

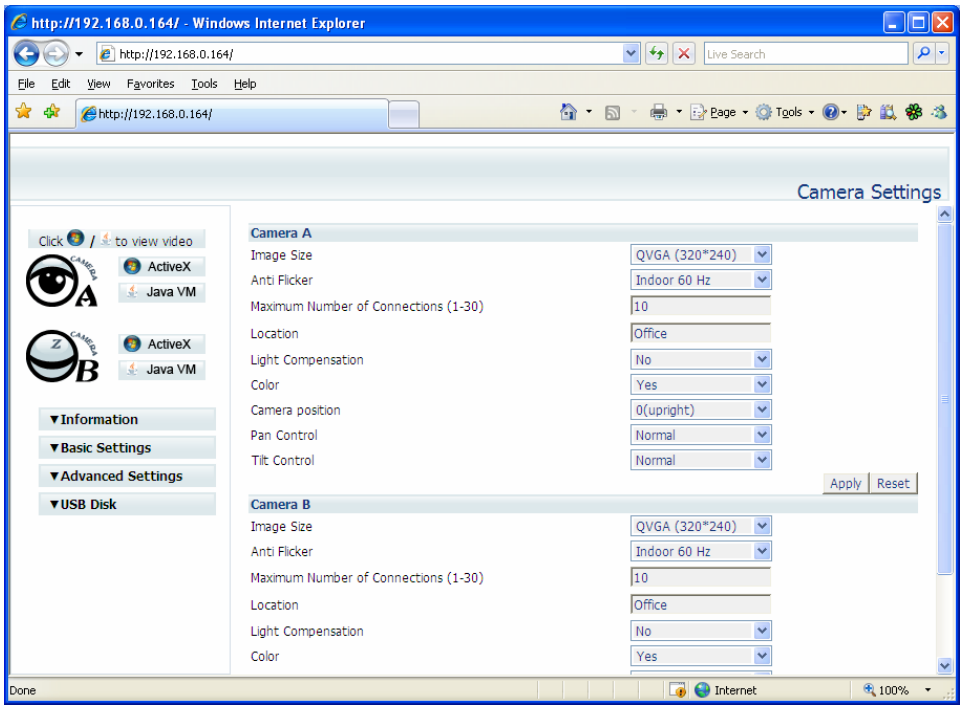


Fig.12 iGuard Web Manager

4.3 IP Configuration

This section allows advanced configuration of IP property.

Select the iGuard on the right display screen, and then click “IP Configuration”. This will bring up the IP Configuration window. There are two tabs;

- IP Address

You can set the camera to “Obtain an IP address by DHCP or alternatively “Using Static IP address”, where the user will have to enter an IP Address, Subnet Mask and Gateway of their choice (refer to Appendix C for IP address explanation). Please refer to Set Wizard.

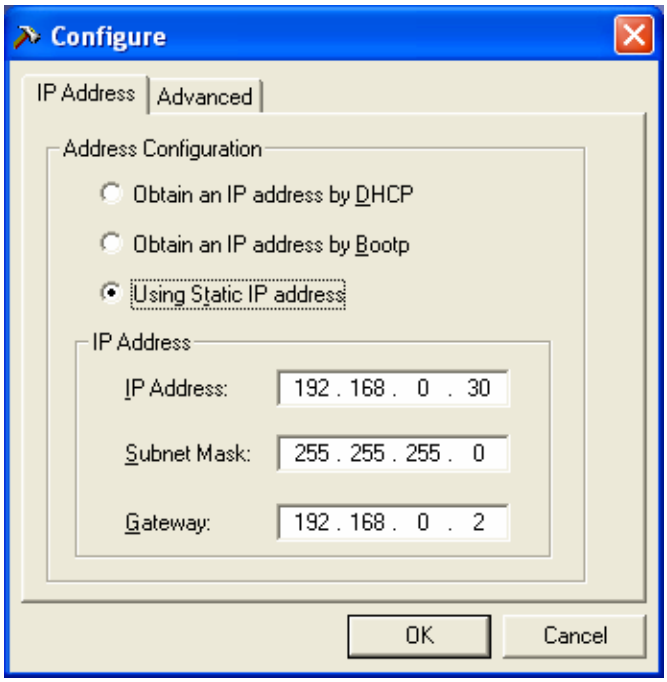


Fig.13 IP Configuration: Set an IP Address for iGuard

- Advanced (for port setting configuration)

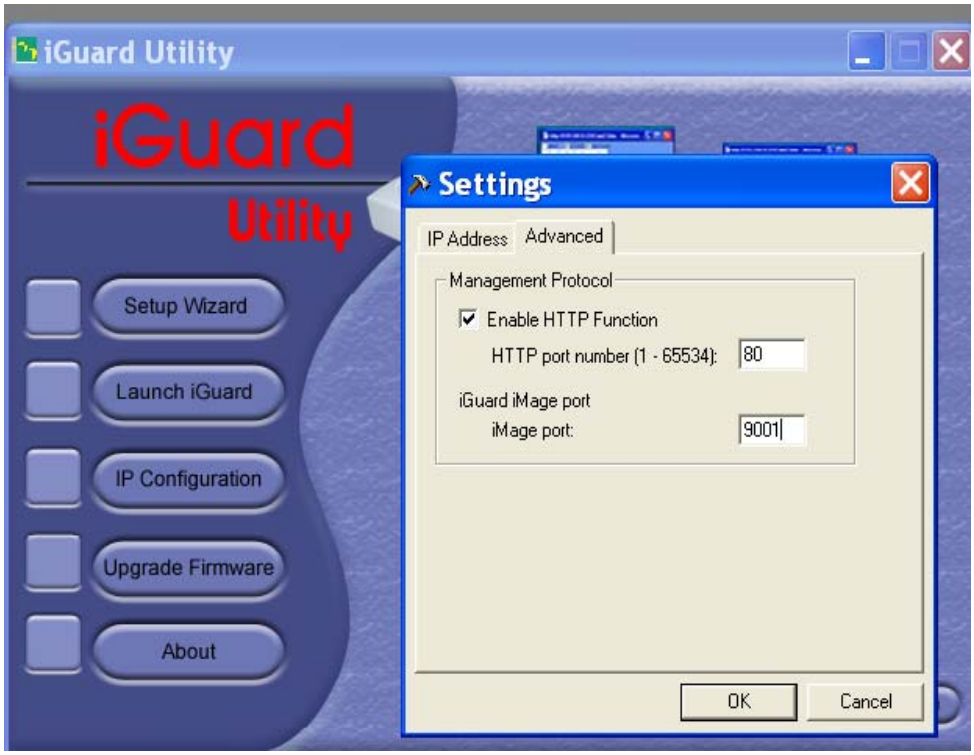


Fig.14 IP Configuration: Port Setting

HTTP Port: You have to enable the HTTP port for the web interface to function. The default values are set to port number 80 for HTTP. Some ISP may block in-bound traffic on port 80 to save bandwidth; or it may have been used by other applications such as website or your router's remote manager, you will have to set a different port for iGuard web manager.

You can disable this port if you wish to deny access to the camera through the web interface and use the iGuardView to view the camera.

Note:

- Once the HTTP port number is set to a port other than 80, the full IP Address must be entered in order to access the web manger. *For example* if you change the HTTP port to 81, then you must enter

  http://192.168.0.177:81

  in the address bar in the browser in order to access iGuard web interface.
- Each iGuard on the local area network (LAN) must have a unique HTTP and UDP port and you have to program your router to forward inbound traffic to these two ports if you wish to access the iGuard from the internet.

UDP Port (image port):.This is the port for the video streaming (uploading). You can change this setting if the default port (9001) is not available (blocked by firewall or used by another device).

4.4 Upgrade Firmware

iGuard Utility offers a convenient method to upgrade iGuard firmware.

1. Click “Upgrade Firmware” to bring up the Wizard.

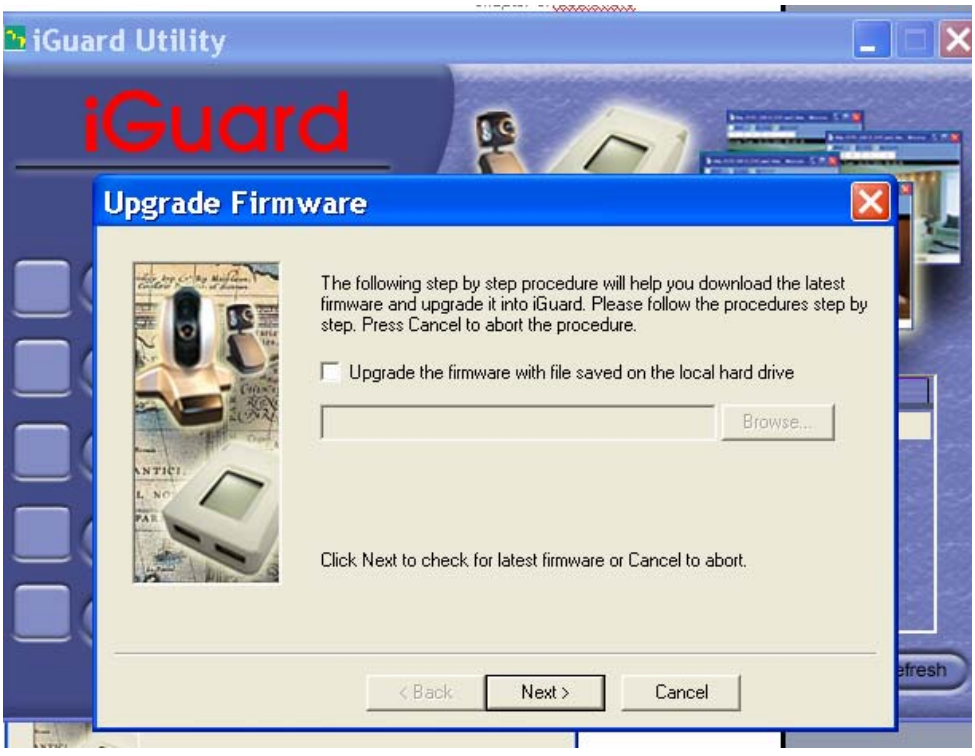


Fig.15 Upgrade Firmware: Updates iGuard firmware

If you have downloaded the latest firmware to your local hard drive, check “Upgrade the iGuard firmware with file saved on the local hard drive” and browse to the file location.

2. Click “Next >” to check for the latest available firmware.

3. Select new firmware file (*.bin) and,

4. Click “Start”.

The iGuard red and yellow LED will flash alternately to indicate that firmware upgrading is in progress. Once completed, iGuard will reboot.

NOTE:
If the downloading / upgrade process is interrupted or the data is corrupted, the iGuard may become non-functional which is not covered by the standard warranty

Chapter 5 iGuard Web Manager

5.1 Introduction

If you have connected the iGuard to an internal network with a DHCP server, the IP property (IP address, Mask, and Gateway) will be automatically assigned, which will be displayed, one group at a time, on the LCD screen of certain iGuard models. In this case, you can access and setup the camera directly through the web interface

1. Start the Web Brower (Netscape or Internet Explore)

2. Enter the iGuard IP Address shown on iGuard's LCD display (e.g. 192.168.0.30) or noted from iGuard Utility and press ENTER.

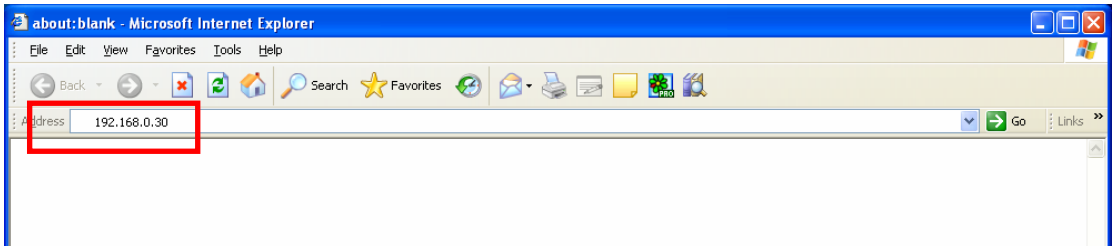


Fig.16 Enter iGuard IP address

3. A login screen will appear. Enter the proper login's and click apply (On firmware V2.52 and later, the default login is not defined, just click on "Apply" to enter the web manager)

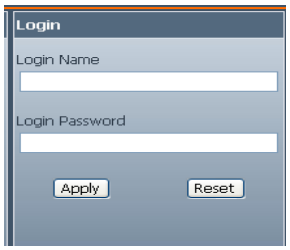


Fig.17 iGuard Login screen

5.2 iGuard Web Manager Interface

The iGuard webpage main menu is divided into two sections. The selection menu on the left and display menu on the right. The selection menu consists of the following options:

- **Web-Camera Selection**
- **Information**
- **Basic Settings**
- **Advanced Settings**
- **USB Disk** (for iGuard 300 series only)

By default the Camera Settings page is displayed when you login. Please refer to 5.2.3.1 to setup the camera.

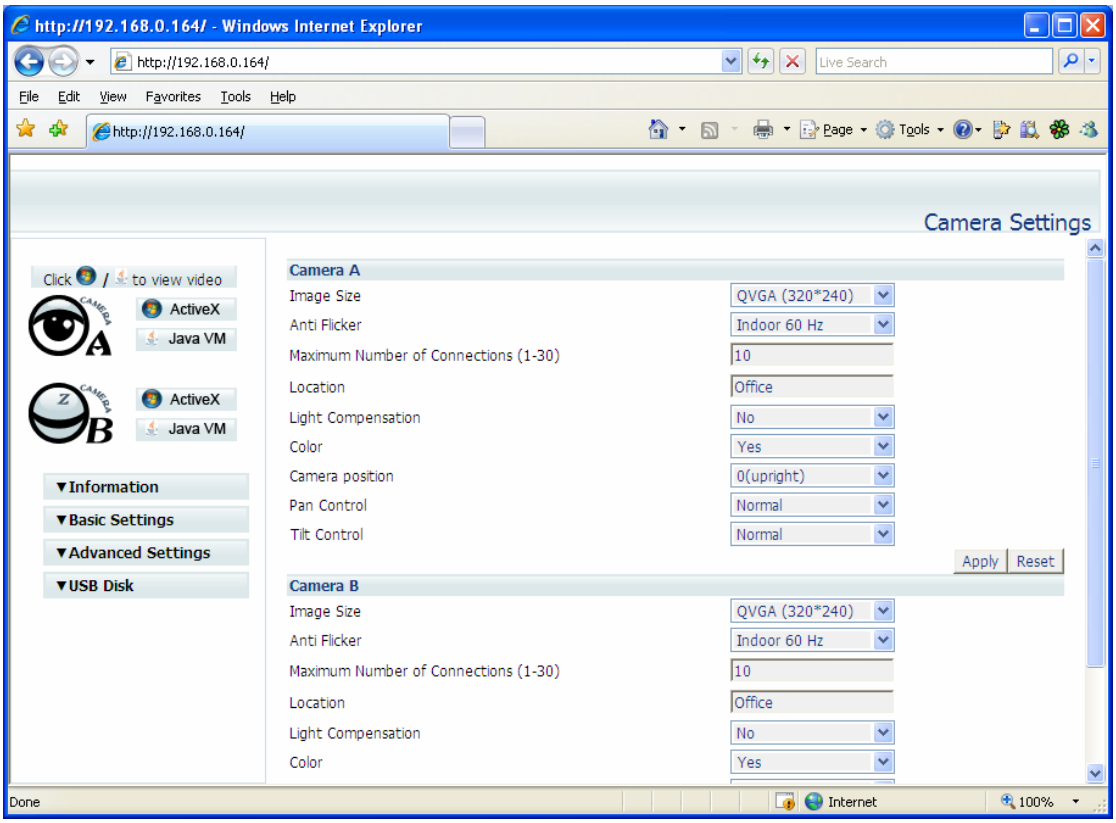


Fig.16 iGuard Web Manager Main Menu

5.2.1 Web-Camera Selection

Click on either “ActiveX” or “Sun Java” from Camera A or B to view the camera images.

By default the first USB camera connected to iGuard will be denote as “Camera A”

5.2.1.1 Video Streaming

If the camera is installed properly, the “Eye” icon will blink. By default the embedded camera will be designated as “A” and the add-on camera will be “B”



Click on “Active X” or “Java VM” icon next to Camera “A “or “B” to view the camera.



Note: ActiveX can only function on Internet Explorer that runs on Windows platform and a plug-in has to be installed on the client's computer. You will have to allow the Active X plug-in in your browser. Alternatively you can use Sun Java to view the video feed. Sun Java also allows users who are not using Windows based Operating System or Browsers other than ***Internet Explorer*** such as ***Fire Fox*** to view the video feed.

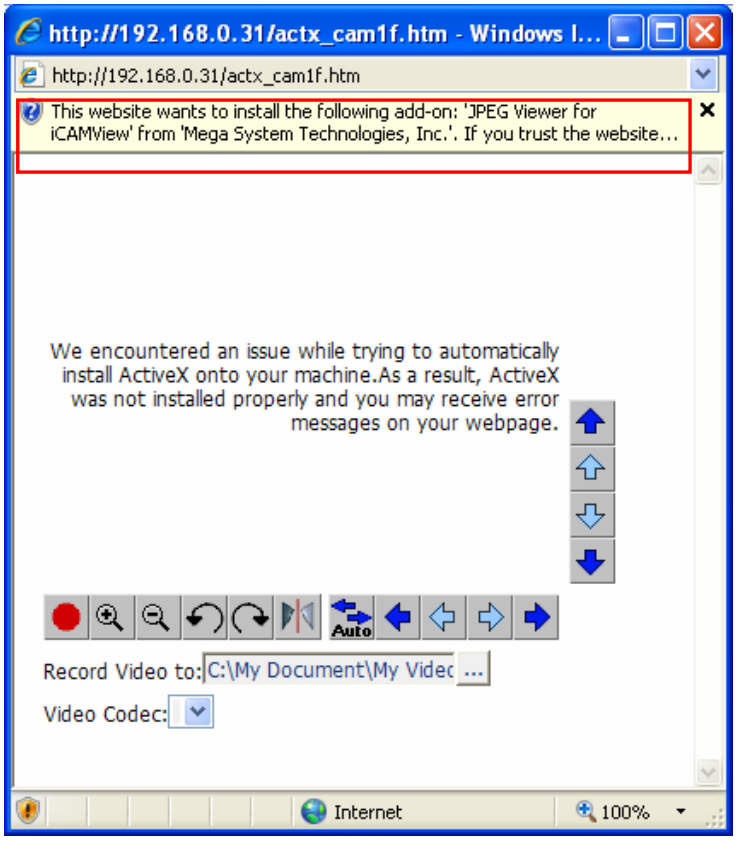


Fig.17 iGuard Plug-in Installation

Once the plug-in is installed the image will appear.

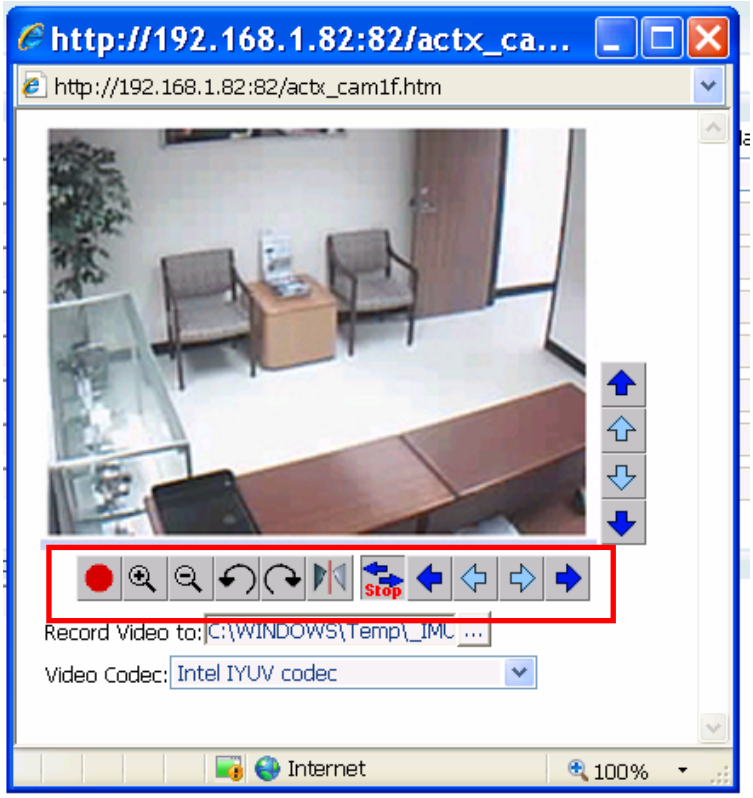


Fig.18 iGuard Camera Window

Make sure to adjust the camera's focus for best picture results.

Click on the controls along the Popup Window to control the functions of the cameras.


Digital Zoom In, Digital Zoom Out


Rotate Left, Rotate Right


Flip the image vertically.



Auto Pan the camera


Pan Left by 5 deg / Pan Left by 1 deg.


Pan Right by 1 deg / Pan Right by 5 deg.

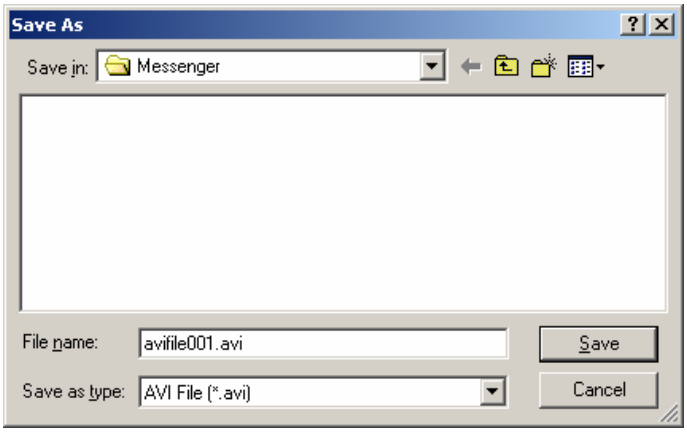

Tilt Up by 5 deg / Tilt Up by 1 deg.


Tilt Down by 1 deg / Tilt Down by 5 deg.



NOTE:
The above Pan/Tilt function will only work with cameras supporting the Pan/Tilt function.

One-Button Recording: Click  to record the video to the selected directory. To change the saved location and filename. Click  and the "Save As" window will pop up. Choose an alternate location and filename. Click the "Save" button to confirm changes.



To change Video Codec, click 

Note: The "Video Codec" pull down will only list the codec that have been installed on your PC. MPEG4 is recommended for the high compression ratio.

Video-Playback: you can use Windows Media Player or any compatible media player to playback the recorded video.

5.2.2 Information

5.2.2.1 System Status

This displays all the information relating to iGuard.

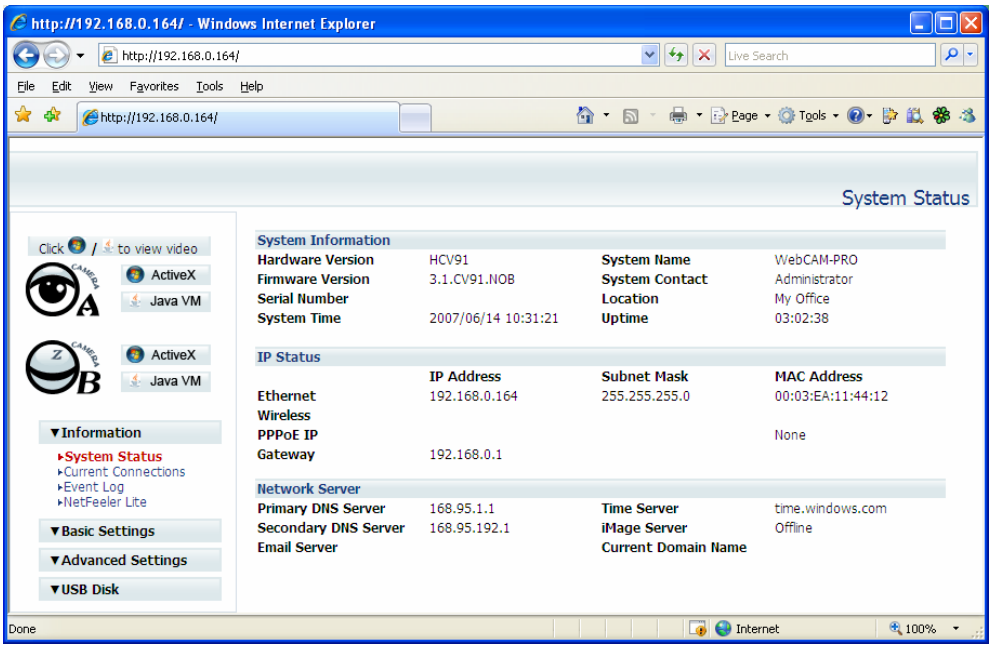


Fig.19 iGuard System Status

i. System Information

This section shows general hardware information such as the Hardware and Firmware Version, the serial number, current / local System Time, the system name, contact, location and uptime.

ii. IP Status

This section shows the network information.

Note: When a wireless dongle is used, there will be two distinct LAN IP's, and MAC address. One for LAN connection, another for Wireless.

iii. Network Server

This section shows mostly 3rd party server information such as the iMage Server, Dynamic Domain Name Server (DDNS) or assigned Email Server.

5.2.2.2 Current Connections

This will show all the users currently viewing either Camera A or Camera B. It also lists, the login time, and total bytes received. The user has an option to block the IP or even disable the account of any errant viewer. The administrator privilege will be required for this feature. A total of 10 connections can be displayed at the same time.

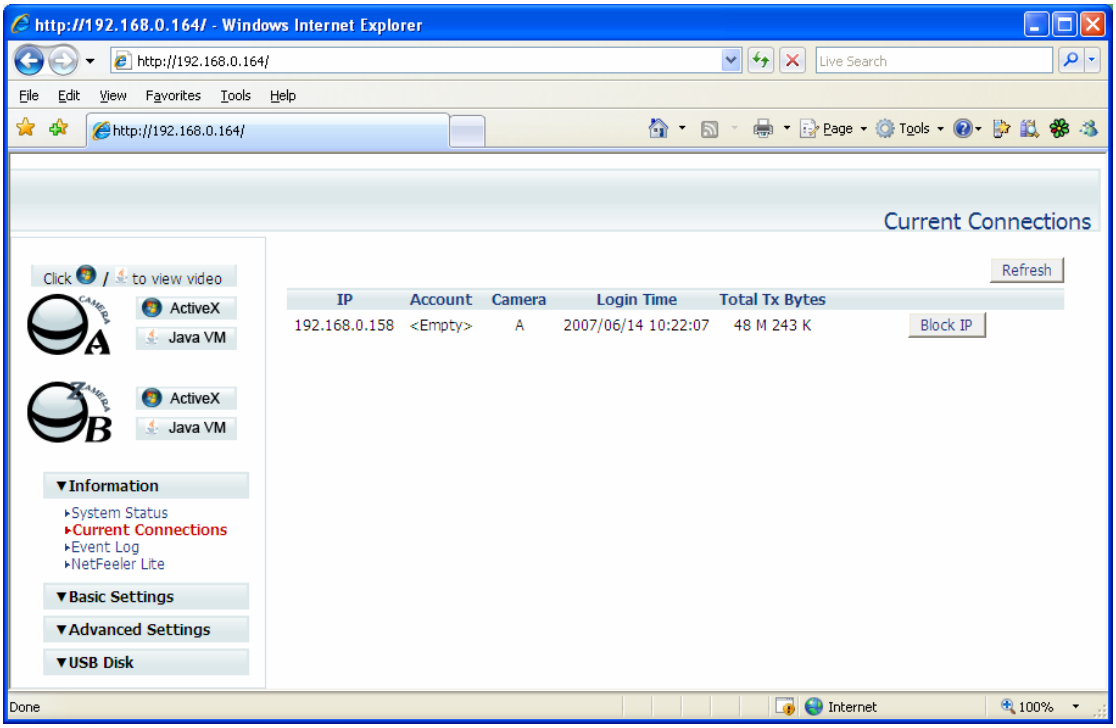


Fig.20 iGuard Current Connections

Note: Administrator privilege is required to view and use **Block IP**. Otherwise, the **IP** and **Account** details will be hidden and **Block IP** function disabled.

IP	Account	Camera	Login Time	Total Tx Bytes	
..*.*	********	A	2007/01/01 00:50:23	40 M 529 K	Block IP
..*.*	********	A	2007/01/01 00:51:36	32 M 242 K	Block IP

Click **Block IP** to block or disable the account of any errant viewer.

To unblock the IP go to **Basic Settings → Account Settings → Blocked IP List** and delete the blocked IP Address from the **Blocked IP List**.

5.2.2.3 Event Log

This section will keep a record of all events that occurred in iGuard. The user can Refresh, Clear or Save the log file. There is also an option to sort the logs according to "Level" or "Type". iGuard can log up to 2,000 events.

Once the number of events has reached the maximum limit, the oldest event will be removed for each new event logged.

Note: If you do not have Administrator privilege, the **User Name** and **IP Address** will be hidden. *Example*: Camera A: user ******** connected from IP: *.*.*.*

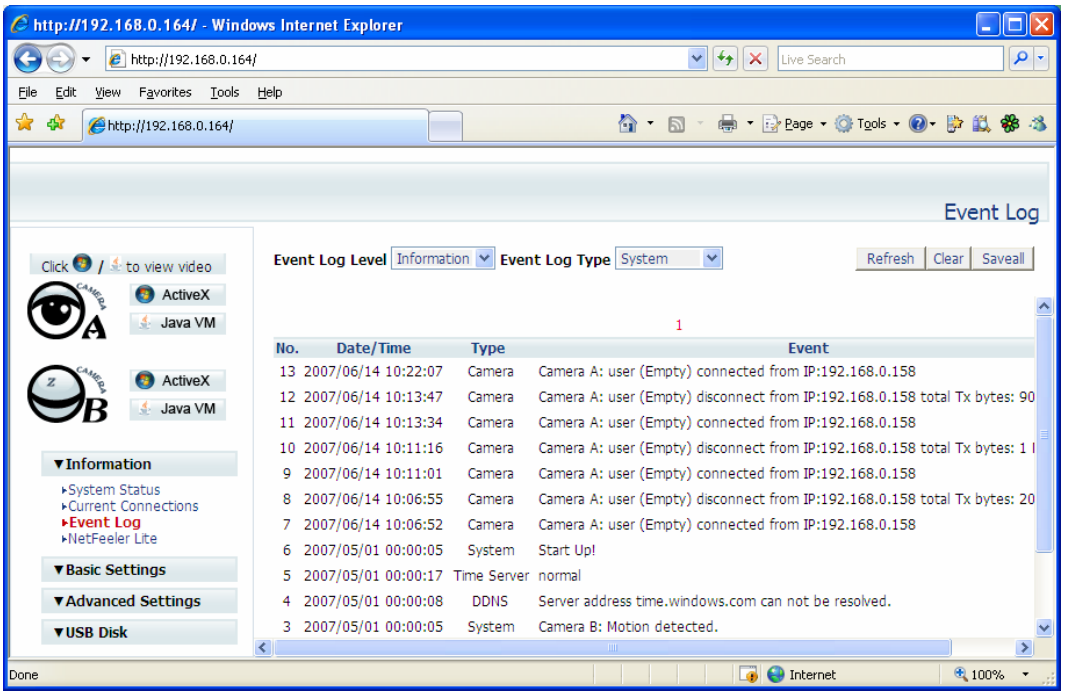


Fig.21 iGuard Event Log

5.2.3 Basic Settings

5.2.3.1 Camera Settings

i. Setting up Camera A (Similar with Camera B)

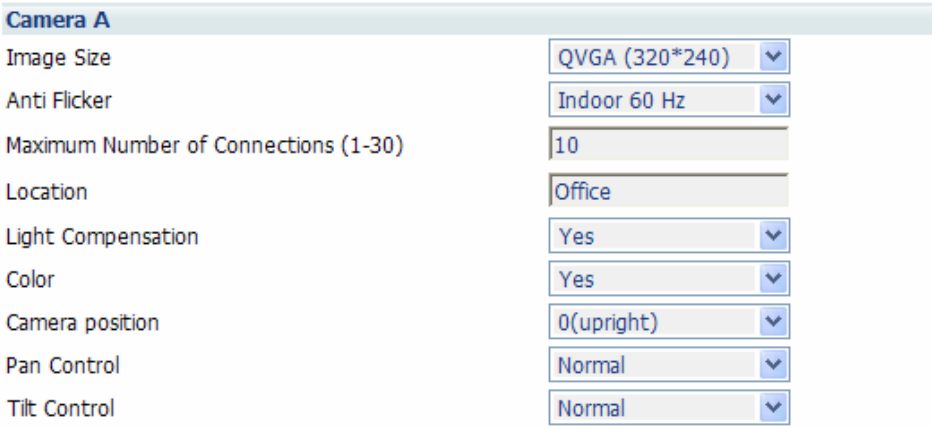


Fig.22 Individual Camera Configuration

"Image Size"

You can set the image size to the following resolutions:

640x480(VGA)
352x288((CIF), supports digital Pan/Tilt
320x240(QVGA)
176x144(QCIF), supports digital Pan/Tilt
160x120 (QQVGA), supports digital Pan/Tilt

"**Anti Flicker**"

Choose between 50Hz, 60Hz or Outdoors.

Indoor 50Hz: for incandescent lights,

Indoor 60Hz: for florescent lights,

Outdoor: for day light or bright light conditions



Note:
If you do not choose the right frequency, the image will flicker or lines will appear on the images, or the images may appear washed out.

"Maximum Number of Connections (1-30)"

Use this to limit the number of users that can connect to this camera. The default is 10. The higher the number the more the bandwidth requirement

"Location"

Enter a suitable location / name to identify the camera.

"Light Compensation"

Choose "Yes" and iGuard will increase the lighting of the image. This is useful when monitoring indoor under low light condition

Choose "No" if you do not want iGuard to adjust the light and view the images as is.

"Colour"

Choose "Yes" for colour and "No" for black and white display. This will help reduce bandwidth requirement

"Camera Position"

Choose from the automatic "0 degree (upright)", to 90, 180 (upside down), and 270 degree position of the camera. This is to facilitate the ability to reposition the camera in any way the user desires.

"Pan"

Choose between "Normal" for regular placement or "Reverse" when the camera is placed upside down.

"**Tilt"**

Choose between "Normal" for regular placement or "Reverse" when the camera is placed upside down.

Click **"Apply"** to save changes. Otherwise, all changes will be lost.

5.2.3.2 Network

This option determines the iGuard Network settings.

i. IP Address

By default, the IP address is set to be automatically assigned by DHCP server. If you have a static IP, you can enter the new address here and click "Apply" to change (Note: you will lose connection to the iGuard if the IP is changed).



Fig.23 iGuard IP Address Settings

"IP Address"

This item determines iGuard IP Address.

"Subnet Mask"

This item sets iGuard Subnet Mask. The value is normally 255.255.255.0

"Gateway"

This item is to set iGuard Gateway.

"Obtain an IP address"

This allows the user to choose either to set iGuard IP Address manually or via DHCP. iGuard will reboot after the above settings have been changed.

ii. DNS Server IP



Fig.24 iGuard IP DNS Server IP

"Primary DNS Server IP"

This item sets iGuard primary DNS Server IP address.

"Secondary DNS Server IP"

This item sets iGuard secondary DNS Server IP address. iGuard will use the secondary DNS Server IP address if the Primary DNS Server IP address is not working.

Note:
You have to set the DNS setting for the FTP and Email notification to work properly.

iii. Port Number



Fig.25 iGuard Port Settings

"**Web Access Port**" (HTTP Port)

By default the port number is 80. You have to use a different port number here if you host a website on the same network, if your ISP blocks port 80 traffic, or if you have multiple iGuard on the network.

If this port is changed, say to 82, then http://xxx.xxx.xxx.xxx**:82** must be used in order to access iGuard's web interface in LAN. (where xxx.xxx.xxx.xxx is the assigned IP address)

"**Video Access Port**" (UDP Port or Image Port)

By default the port number is 9001. You have to use different UDP port for each iGuard if you have multiple iGuard on the network

iv. Ethernet



Fig.264. iGuard Ethernet Settings

"**Connection Type**"

This item sets the communication speed between iGuard and the Network. iGuard will reboot after "Connection Type" is changed.

v. Dynamic DNS

If you use a consumer grade broadband service, the chances are you will have a dynamic IP address. You will need to subscribe to a DDNS service to keep track of this ever-changing IP address if you would like to use the remote monitoring function of iGuard.



Fig.27 iGuard Dynamic DNS Settings

As value added service, iGuad.com hosts a DDNS server that tracks iGuard's IP address if it was changed for any reason. Before you use this function, you will have to open an account on iguard.com:

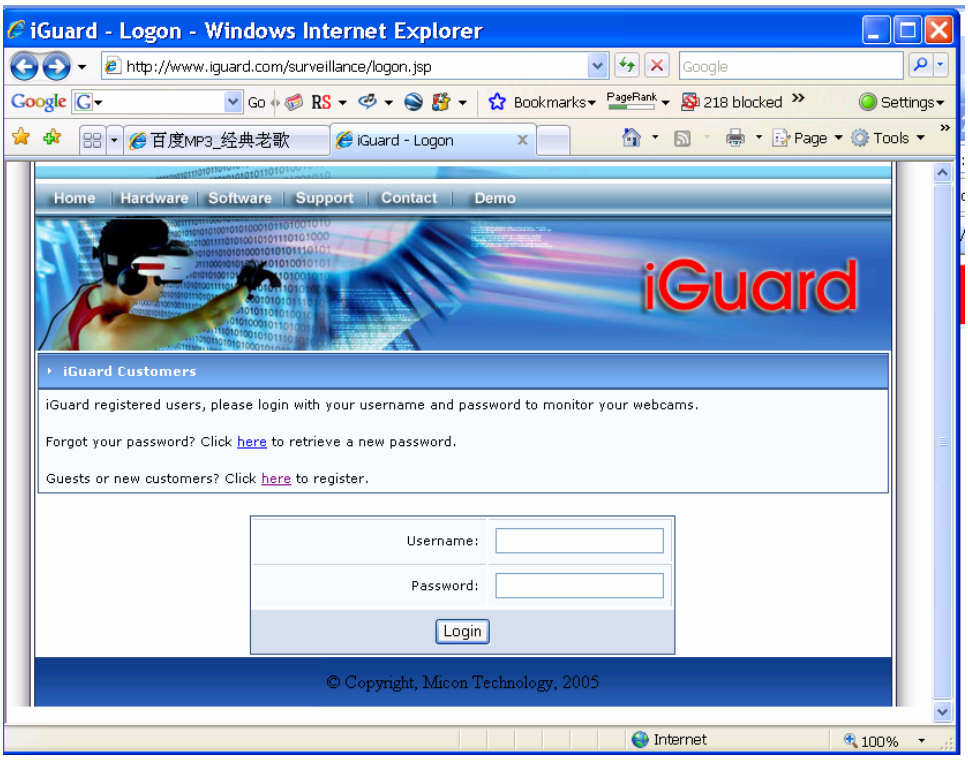


Fig.28 iGuard DDNS Service Sign Up

Once you set up the account, you can then add all the cameras to your account:

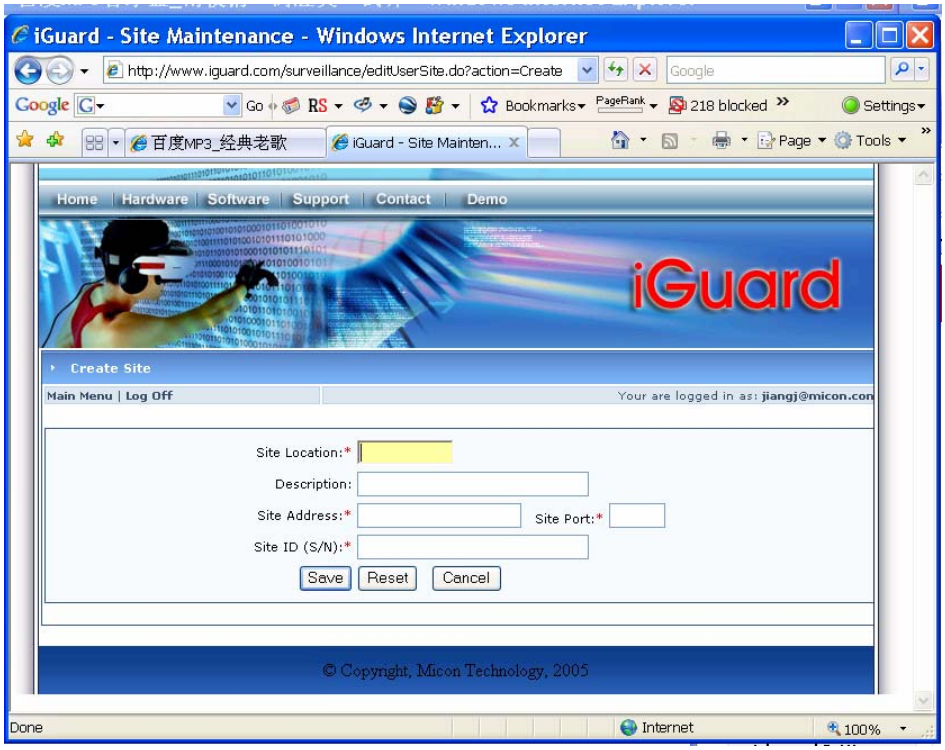


Fig.29 Register Camera

From now on, you can then access all your cameras from iGuard.com

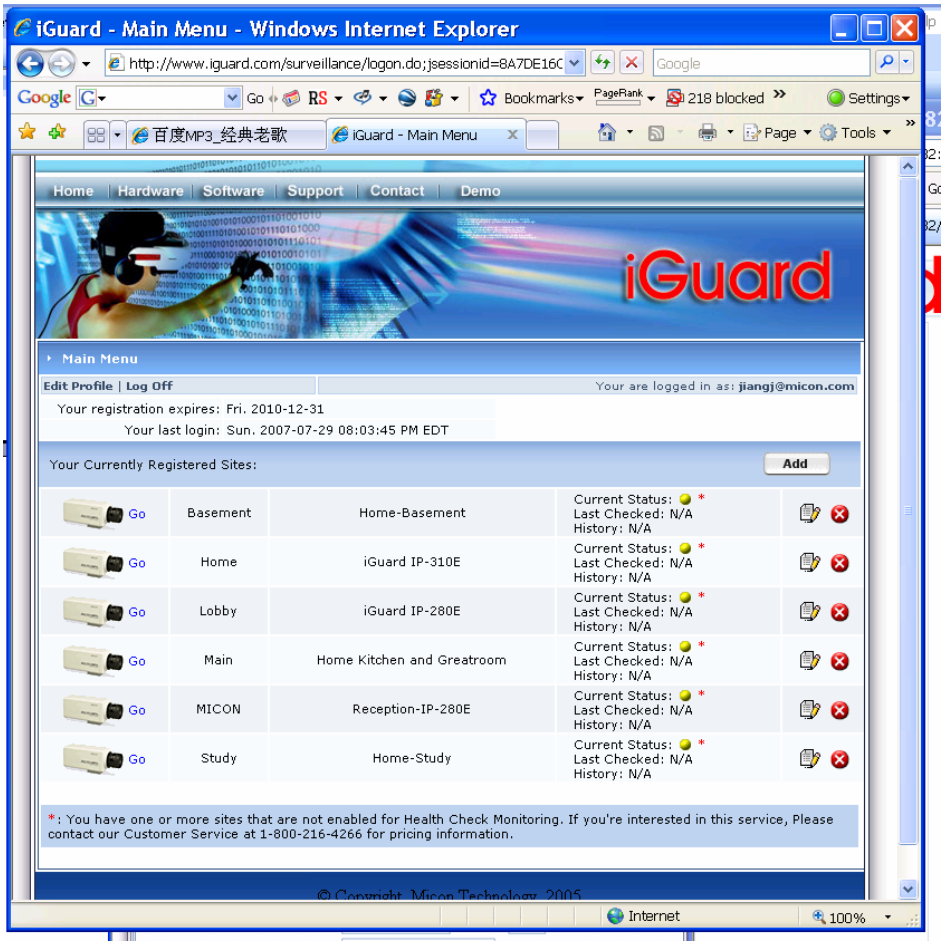


Fig.30 iGuard Camera List

vi. PPPoE

If you use a dedicated DSL internet service, use this option to set up the camera to directly dial-up your DSL modem and connect to the Internet.



Fig.31 iGuard PPPoE setting

"**When Connection should be made**"

The user has a choice of;

Disabled	:	Default setting. iGuard does not dial in
Connect always	:	iGuard will automatically dial in.

"**Login Name**"

Enter the login name assigned by your ISP.

"**Login Password**"

Enter the password assigned by your ISP.

5.2.3.3 Wireless Setting

This option is only configurable if a compatible wireless USB dongle is attached. To set this up, you'll first need to use the LAN IP (as shown on iGuard Utility) to access the camera.

Note:
Once the wireless configuration is setup, the wireless IP address will be shown on the LCD instead of the LAN IP. To check the LAN IP thru the LCD, unplug the wireless USB dongle.

i. Wireless

Connect a compatible Wireless USB dongle to enable this feature.

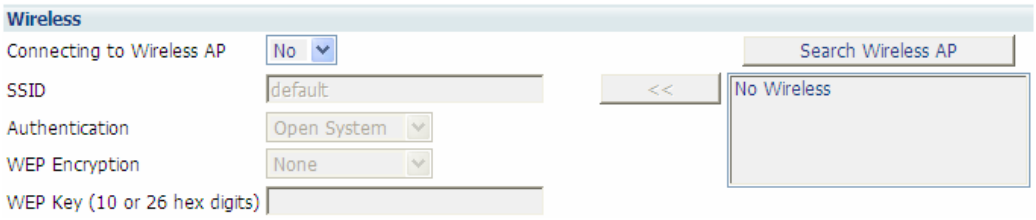


Fig.32 iGuard Wireless Setup

Connect to Wireless AP

When a compatible Wireless USB dongle is connected, select **Yes** and click **Search Wireless AP** button to have it search for nearby Access Points (AP).

Once detected all available AP will be displayed on the table to the right. Select the preferred AP and click **<<** button to add it to the **SSID** field.

Authentication

Select either; Open System or Shared Key. Check the AP for the appropriate authentication method in use.

WEP Encryption

Select from either; none, 64-bit key or 128-bit key. Check the AP for the appropriate encryption used.

WEP Key (10 or 26 hex digits)

Key in the password used

ii. IP Address

Refer to section 5.2.3.3 (i) above. This will be the ***wireless*** LAN IP. It will be different from the LAN IP.

iii. DNS Server IP

Refer to section 5.2.3.3 (ii) above. This will be the ***wireless*** DNS server IP. It can be different from that of the LAN IP.

5.2.3.4 Account Settings

This allows you to set up to Eight (8) user account with different permissions for iGuard.

WARNING: You **MUST** set an Administrator account **BEFORE** setting either "Operator", "Viewer" or "No Access". Failure to do so will result in you being locked out of iGuard Web Manager! You will have to refresh your firmware to be able to use the iGuard again

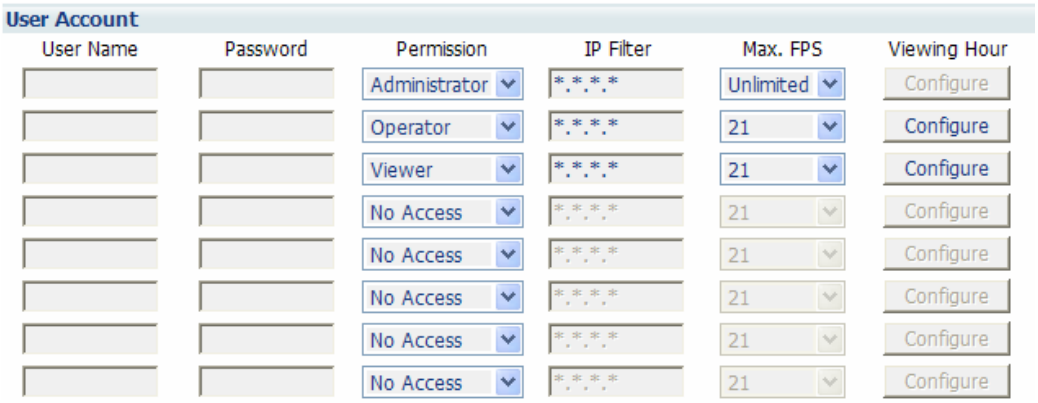


Fig.33 iGuard User Account Setting

i. User Account

"User Name"

Determine the username of visitors who can log in. The administrator can set a name consisting up to 32 case sensitive characters

"Password"

Set a password for the visitor's account. The administrator can set the password with up to 32 case sensitive characters.

"Permission"

Determine the permission level to one of "Administrator", "Operator", "Viewer" or "No Access"

Administrator:	This permission allows the user full access including write permission to all the sections.
Operator:	This permission level allows the user access to iGuard menus, but without the permission to amend them. The administrator can also set "Permit Hours" here for seeing camera.
Viewer:	This permission level allows the user to access iGuard at specific time as set in "Permit Hours" for seeing camera. The user does not have write permission and only access the "Web Cam" and "Information" section.
No Access:	This is to revoke either of the above two permission levels given to a user. And make the user account disable.

Note:
An **Administrator** account must be set before setting up either an **Operator** or **Viewer** account. An administrator account fields, in this case, cannot be left empty.

"IP Filter"

Visitor can only login from the IP address specified here for security consideration. You can restrict a user access only from 192.168.1.0/24 by setting up "192.168.1.*". Otherwise, leave it as "*.*.*.*" to allow the user to login from any place.

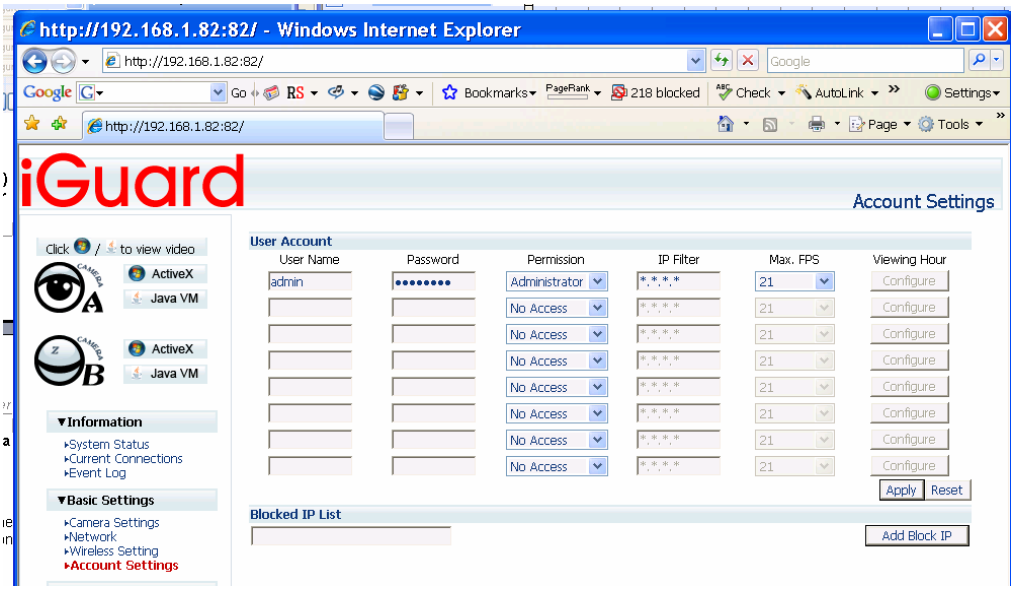


Fig.34 iGuard User Account Settings

"Max FPS"

This allows the administrator to determine the frames per second ("FPS") allocated to each type of account. By limiting the FPS, the administrator can manage the limited bandwidth available. The administrator can set a figure between 1 to 30 and unlimited FPS.

Note:
This is the maximum frame rate that can be achieved if all the available resources are allocated to the user. In reality, the user will experience less frame than specified.

"Permit Hours"

When the Permission level is set to either "Operator" or "Viewer", the Administrator can configure and determine the time to which either permission level can access the camera.

Click "Configure" to bring up the following window. You can set up to 4 different Permit Hours (in 24hr format). Click "Apply" to save and "Close" to exit.

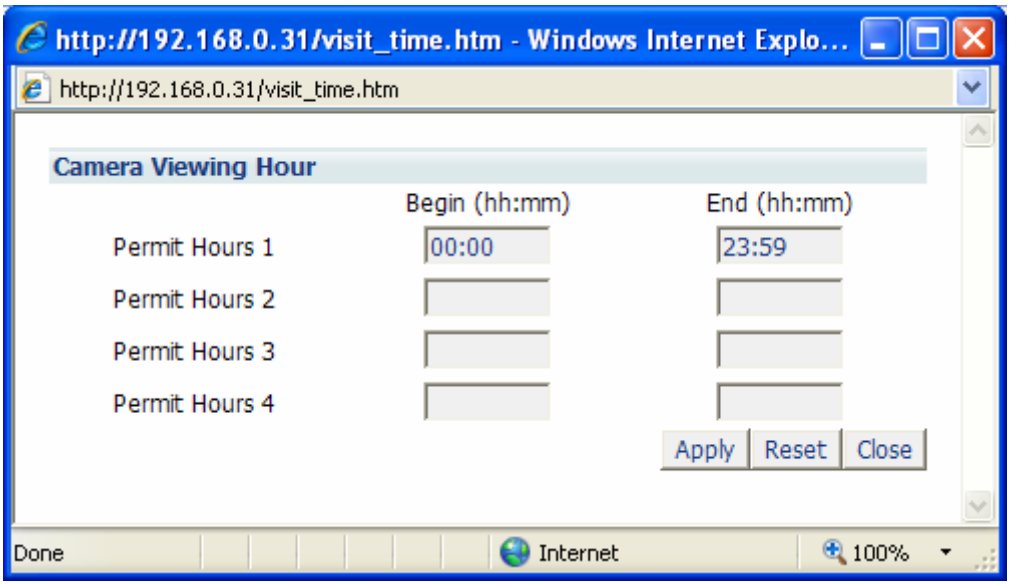


Fig.35 iGuard Permit Hours Configuration

5.2.4 Advanced Settings

5.2.4.1 Event Notification

This determines the type of event an email is sent by iGuard. iGuard can send notifications to up to 8 email recipients. Note: You must have Administrator privilege to edit this section.

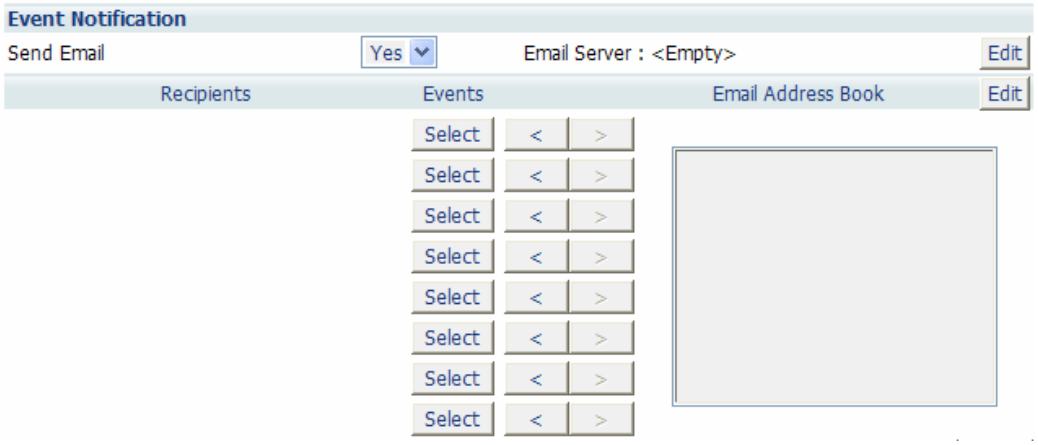


Fig.36 iGuard Event Notification Page

i. Event Notification

"Send Email"

To activate Event Notification, you will need to set "Send Email" to "Yes". Select "No" if you do not wish to send out any notification.

"Email Server"

A valid "Email Server" with username and password (if authentication is required) must be made available for this feature to work. If you do not have this setup, or wish to change the settings, click on "Edit".

Note:
Email function can only work using standard Email Server and not Web based Email Server, such as yahoo.com / msn.com.

"Email Address Book"

The available Email addresses are listed here. Refer to section 3.2.4.3 on how to enter an Email address to the **Address Book**.

To add an email address not already in the list, click **Edit**. iGuard will ask you to save your configuration prior to leaving this page.

"Recipients"

iGuard can send email notification to up to 8 valid email accounts. To add an email to the recipient list, click < . To remove, click > .

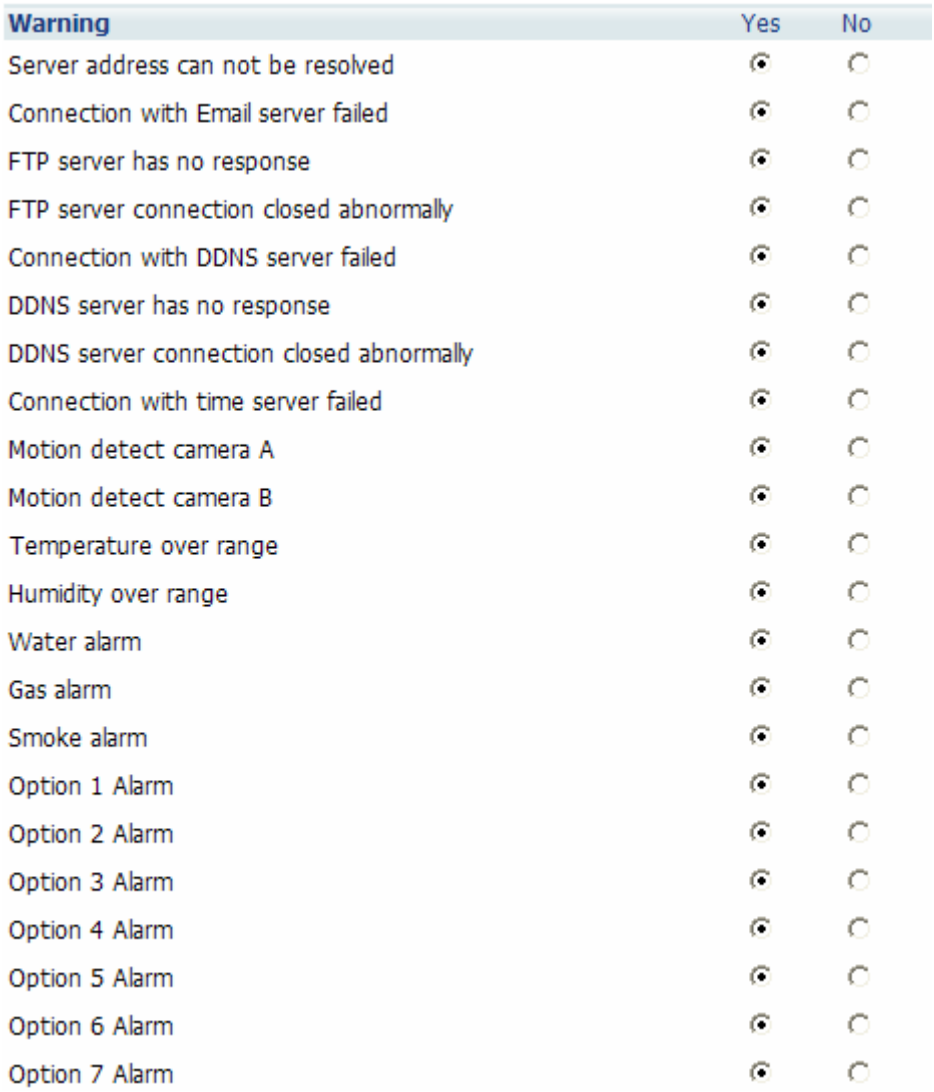
"Events"

This determines the events that the selected recipients will be notified of by email.

There are three types of events, Information, Warning and Error. Click Select to select from the list of events you wish these recipients to be notified of.

Information	Yes	No
Start up	◉	○
PPPoE connection successful	◉	○
Registration with DDNS server completed	◉	○
User logged in to view camera	◉	○
User logged out from camera	◉	○
Image recording of camera A	◉	○
Image recording of camera B	◉	○

Error	Yes	No
Server address was not specified	◉	○
Invalid username or password entered for FTP server	◉	○
FTP server no such file or directory	◉	○
Invalid username or password entered for DDNS server	◉	○
Registration with DDNS server failed	◉	○
DDNS domain name does not exist	◉	○



Warning	Yes	No
Server address can not be resolved	◉	○
Connection with Email server failed	◉	○
FTP server has no response	◉	○
FTP server connection closed abnormally	◉	○
Connection with DDNS server failed	◉	○
DDNS server has no response	◉	○
DDNS server connection closed abnormally	◉	○
Connection with time server failed	◉	○
Motion detect camera A	◉	○
Motion detect camera B	◉	○
Temperature over range	◉	○
Humidity over range	◉	○
Water alarm	◉	○
Gas alarm	◉	○
Smoke alarm	◉	○
Option 1 Alarm	◉	○
Option 2 Alarm	◉	○
Option 3 Alarm	◉	○
Option 4 Alarm	◉	○
Option 5 Alarm	◉	○
Option 6 Alarm	◉	○
Option 7 Alarm	◉	○

Fig.37 iGuard Event Selection List

By default, all the events are selected; you must click “Apply” to activate them. Close the window to return to the Event Notification Page. Click “Apply” to save your settings.

iGuard will send you the following email notification depending on which event you have selected.

Note:
The Image Recording and Motion Detection notification function here will only send an email notification WITHOUT any picture attached. For email notification with images, the Administrator has to setup the **Motion Detection** and **Image Recording** page (see Section 3.2.4.2)

Samples;

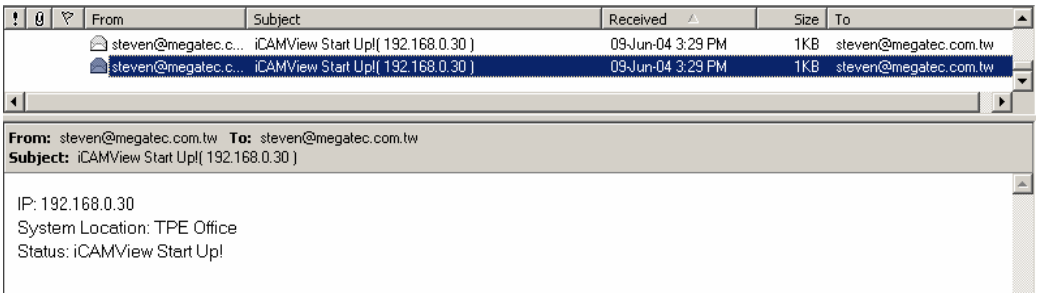


Fig.38 iGuard Event : Start Up

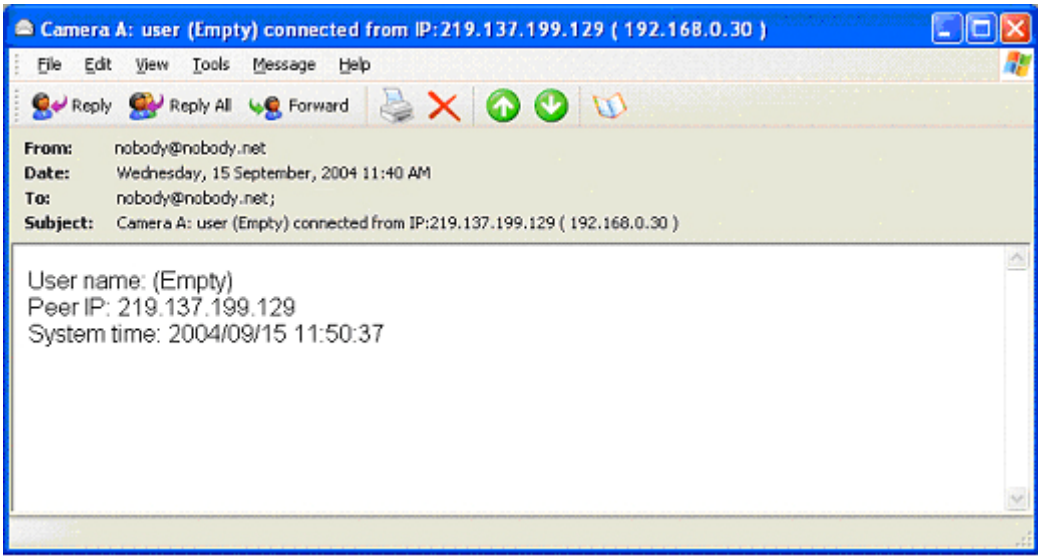


Fig.39 iGuard Event : User Login Details (Date, Time, Camera & IP)

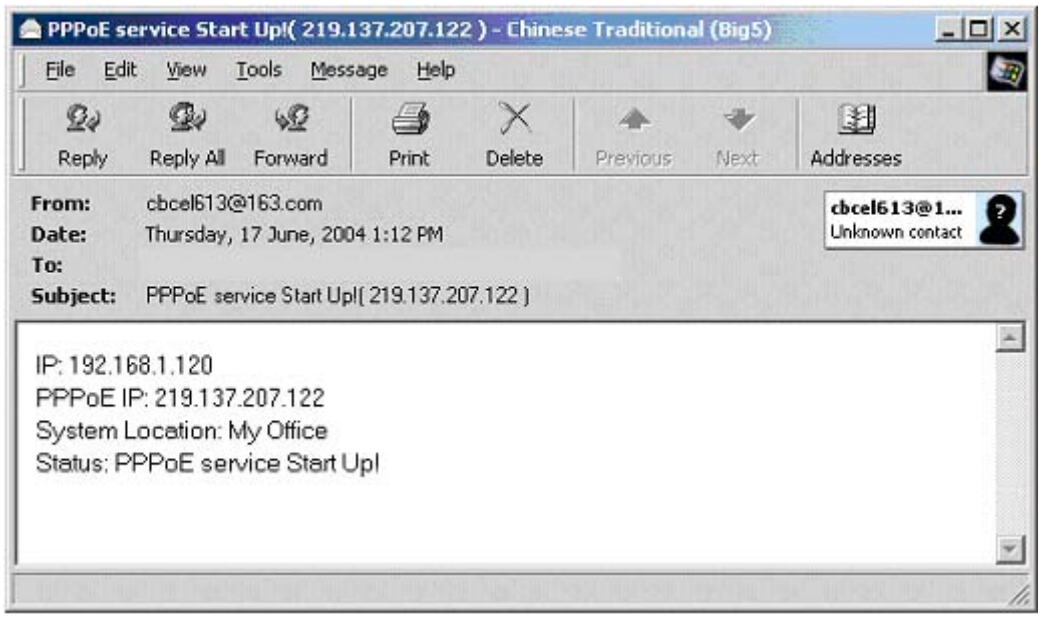


Fig.40 iGuard Event : PPPoE Connect Successful

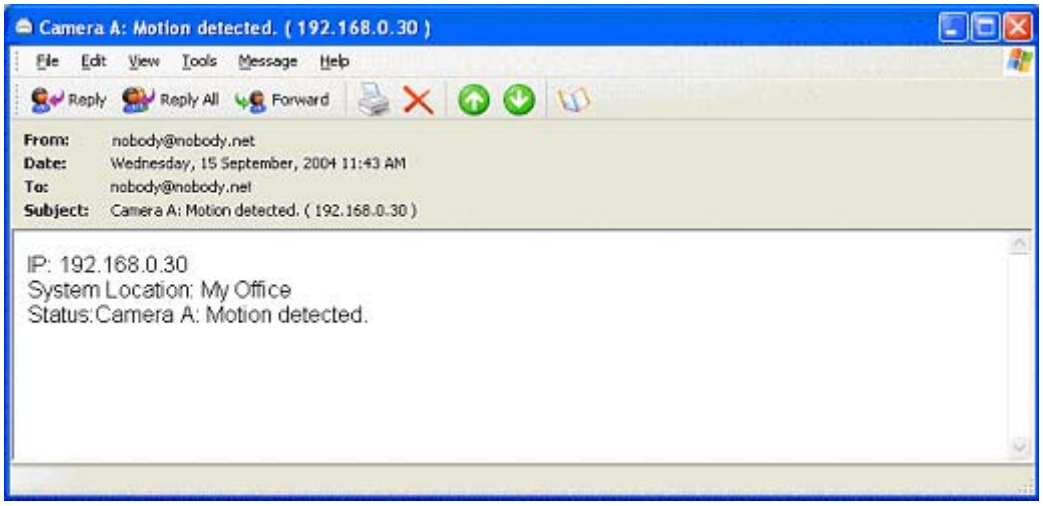
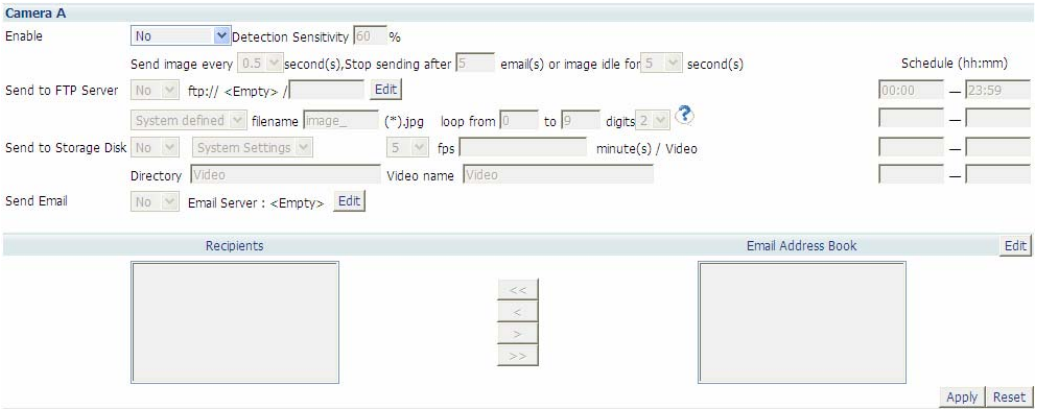


Fig.41 iGuard Event : Camera A or B Motion Detected

5.2.4.2 Motion Detection

This page allows the administrator to set motion detection functions for the cameras.



i. Camera A (or Camera B)

Enable

You have three options for Motion Detection;

a. **Always On,** or;

b. **On Schedule**, the Administrator can set up to 4 different time slots for motion detection, or;

c. **No** to turn Motion Detection function off.

Note:
Check that you have setup valid **Email / FTP** accounts first before proceeding with the rest of the configuration.

To setup **Email / FTP**, refer to Section 5.2.4.3

Detection Sensitivity

This will determine the level of change before motion capture is triggered. A high percentage means a small change will trigger motion capture.

Send image every … second(s)

Select either; 0.5, 1, 2, 3, 4 or 5 seconds.

Stop sending after … email(s) or image idle for … second(s)

iGuard will stop sending emails on the lower of the two conditions. You can set between 1, 3, 5, 7 and 10 seconds. Emails can be set from 1 to 99999 pieces or 0 for stop sending email only when image idle occurred.

Schedule (hh:mm)

When the option is set to **On Schedule**, you can configure the four preferred schedule time slots for motion detection. Time must be entered in 24hr format.

Send to FTP Server

Click **Yes** to activate. This option allows you to send and store the motion detected images on a FTP site. This is useful for future reference and recording purpose.

ftp://<empty>/<folder>

This will set the folder where the Motion Detected files are stored. Enter a folder name in **<folder>**. Click **Apply** when done.

Note:
The folder name must be valid and has appropriate upload permissions.

You must first enter a valid FTP address in **Email / FTP** page. Otherwise the FTP address field will be left **<empty>**.

To setup the FTP server, see Section 3.2.4.3

System Defined / User Defined

You can also determine to either have the system automatically assign the filenames for the pictures saved. Or manually assign the filename.

Filename …

Specify a prefix filename for the motion detected JPG images. The default prefix is **image**_

Loop from … to …

This will determine the number of files in the sequence. Once the last file number is reached, it'll loop and replace the first file in the sequence with the most current image.

Digits …

This will determine the number of digits assignable for the above sequence. You can choose to assign between **1** to **6** digits.

Click  for an example.

Send to Storage Disk

Select **Yes** to save the images to a USB Flash Disk. This function only works if a compatible USB Flash Disk is attached.

Note:
Not all USB external storage devices are compatible. Please test the device before final use. All drives need to be formatted in FAT32.

System Settings / User Settings

You can also determine to either have the system automatically assign the filenames for the pictures saved. Or manually assign the filename.

FPS … minute(s) / video

Specify how many frames per second to record.

Directory / Video name

Use these fields to assign the directory and individual Video file names.

Send Email

Select **Yes** to send an email when motion is detected.

Note:
The received Email / FTP size depends on the resolution set in **Basic Settings → Camera Settings → Image Size**

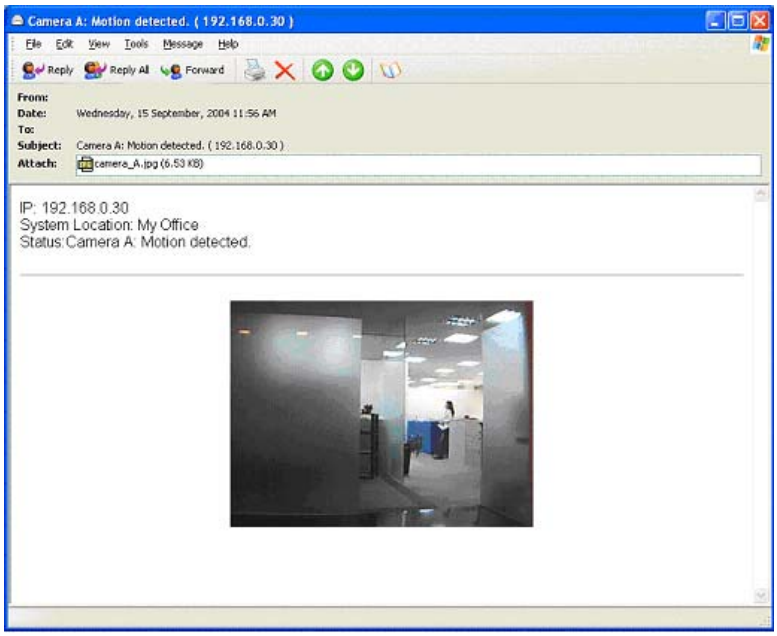


Fig.42 Motion Detect Email Notification

Email Server: …

The Email server will be shown here. If not, click **Edit** to go to the **Email / FTP** configuration page. Click on **Motion Detection** to return here. (refer to section 5.2.4.4 on Email / FTP configuration)

Email Address Book

The available Email addresses are listed here. Refer to Section 5.2.4.4 on how to add an Email address to the **Address Book**.

Recipient

You can determine who will receive email notification.

To add a recipient to the list, click **<**

To add all the recipients to the list, click **<<**

To remove a recipient from the list, click **>**

To remove all the recipients from the list, click **>>**

Click **Apply** to confirm and save the settings.

5.2.4.3 Scheduled Recording

This page allows you to setup Scheduled Recording function for the camera. This function allows the user to receive a string of JPG images to either their email or FTP account or as MJPEG to a USB storage disk. The images will be sent over a predetermined interval

i. For Camera A (or Camera B)

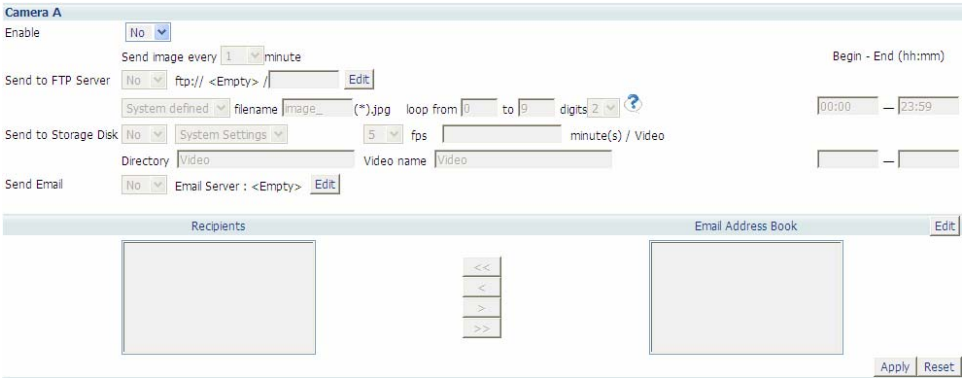


Fig.43 Scheduled Recording webpage

Enable

Click **Yes** to activate this feature.

Begin – End (hh:mm)

You can determine up to 2 different time slots for Image Recording. The time is in 24hrs format.

Send image every … minute(s)"

You can determine the interval (between 1 to 99 minutes) at which iGuard captures and sends an image.

Send to FTP Server & **Send Email & Send to USB Storage Disk**

This is similar to the function available in **Motion Detection** page. Please refer to part (i) above for details.

Note:
The image size received by email / FTP from depends on the resolution set in **Basic Settings → Camera Settings → Image Size**

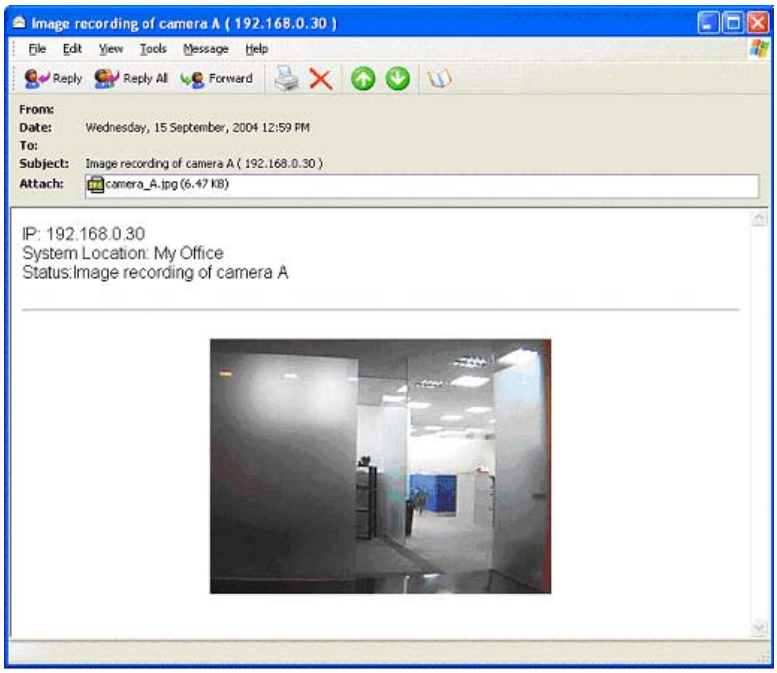


Fig.44 Email of Image Recorded

5.2.4.4 E-mail / FTP

This sets up the necessary Email and FTP server information. You will have to enter a valid Account Name and Password to the Email server and/or FTP server. This information is necessary to allow email notification and ftp file sending features in Advanced Settings.

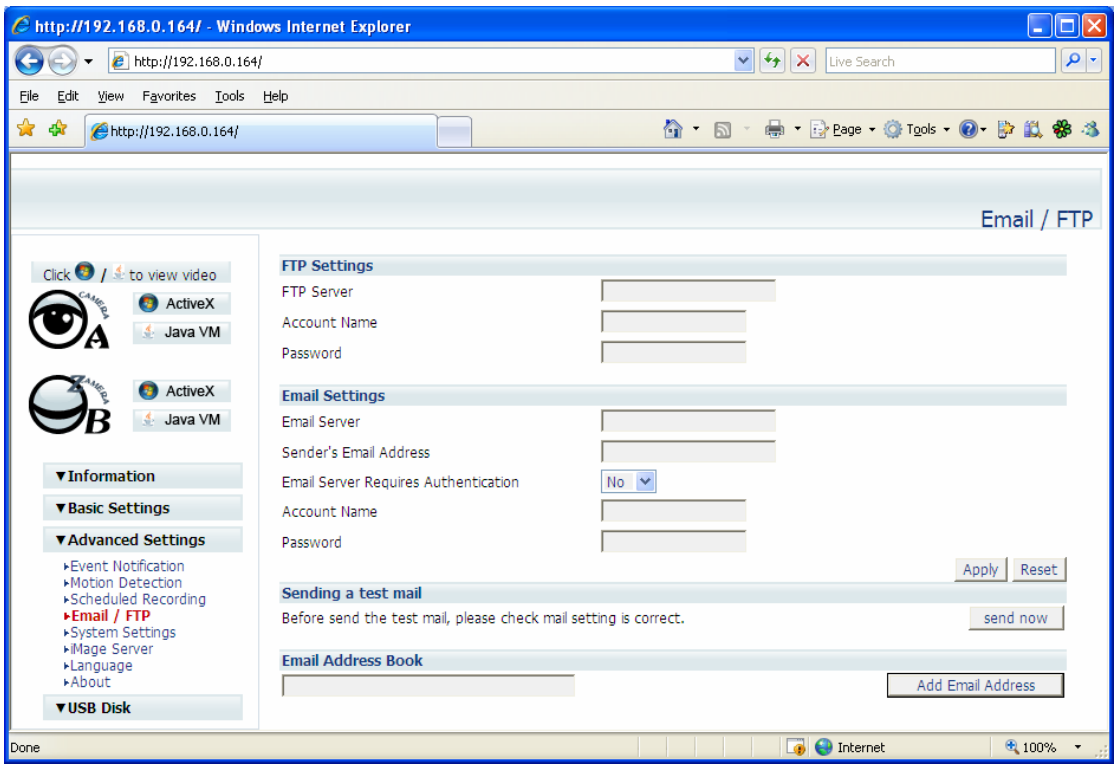


Fig.45 iGuard Email / FTP Page

i. FTP Settings

"FTP Server"

You will have to enter the FTP server address here.

"Account Name"

Enter the FTP account name here.

"Password"

Enter the corresponding password.

Click **"Apply"** to save the above settings.

ii. Email Settings

"E-mail Server"

You will have to enter the Email server address here.

"Sender's Email Address"

This will determines iGuard's Email address.

"Email Server Requires Authentication"

If set to "YES", you will have to provide the account name and password in order to access the Email server. Otherwise, enter "NO".

"Account Name"

Enter the account name or login name to the Email server.

"Password"

Enter the password for the above account name.

Click "Apply" to save the above changes.

iii. Sending Test Mail

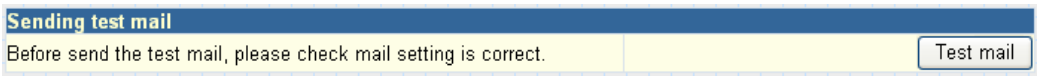
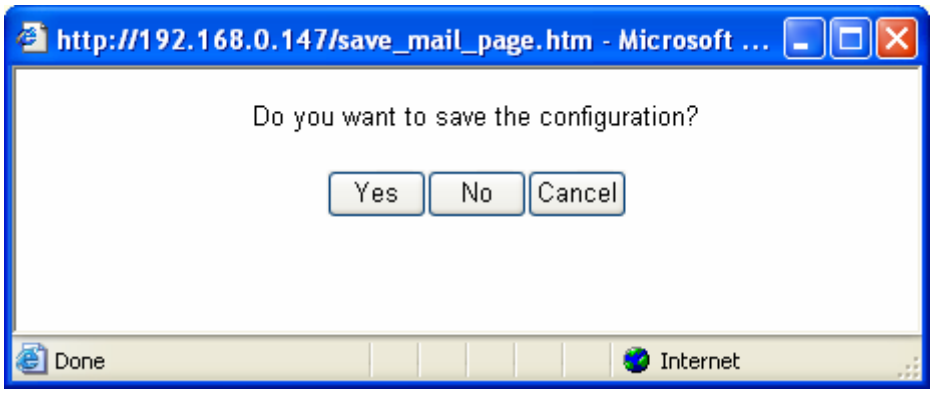
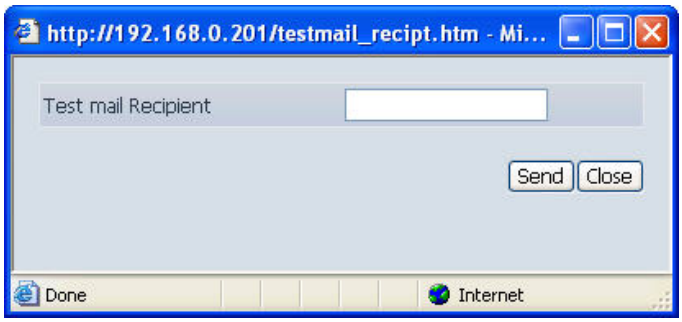


Fig.46 iGuard test mail function

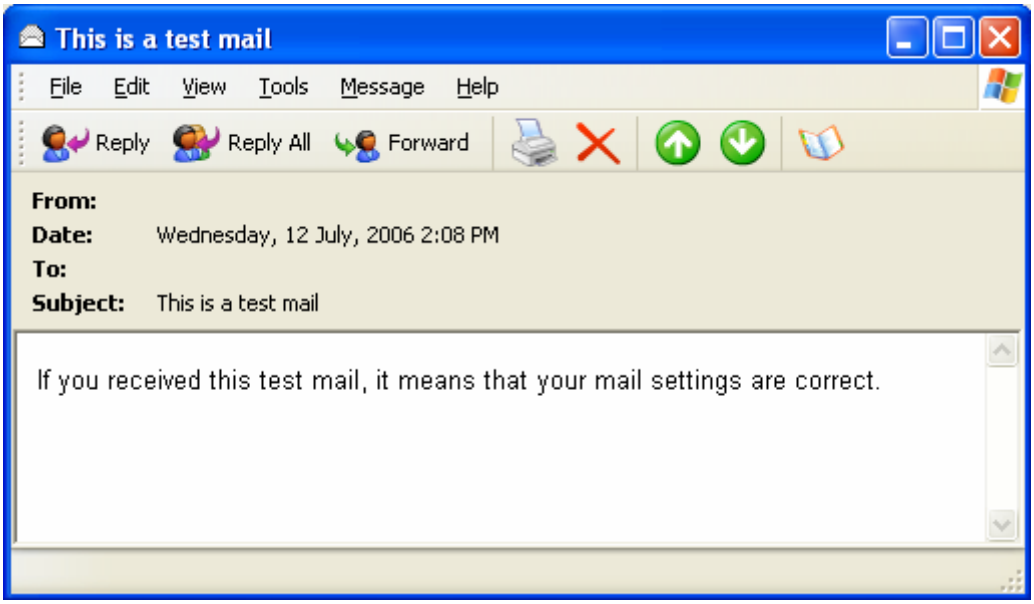
You must have the "Email Setting" configured to proceed with "Test Mail". Once that is done click "Test Mail" and the following will appear.



Click “Yes” to confirm sending and the following window will appear.



Enter the “Test mail Recipient” email address and click ”Send”. If the Test Mail is successful, you’ll receive the following email message;



iv. Email Address Book

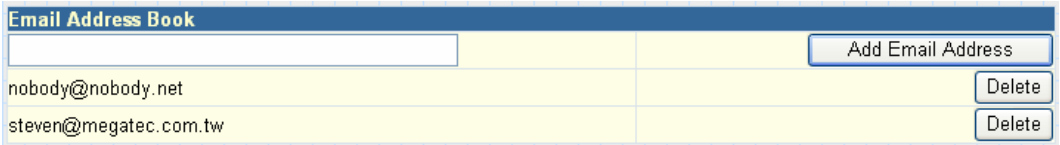


Fig.47 iGuard E-mail Address Book Entry

Enter an Email address in the box provided and click “Add Email Address”. The new email address will be added to the list. You can store up to 20 email addresses here.

To delete an Email address, just press “Delete”.

5.2.4.5 System Settings

This page allows you to set iGuard SNMP settings so it can be used by a NMS (Network Management System) like iGuardView.

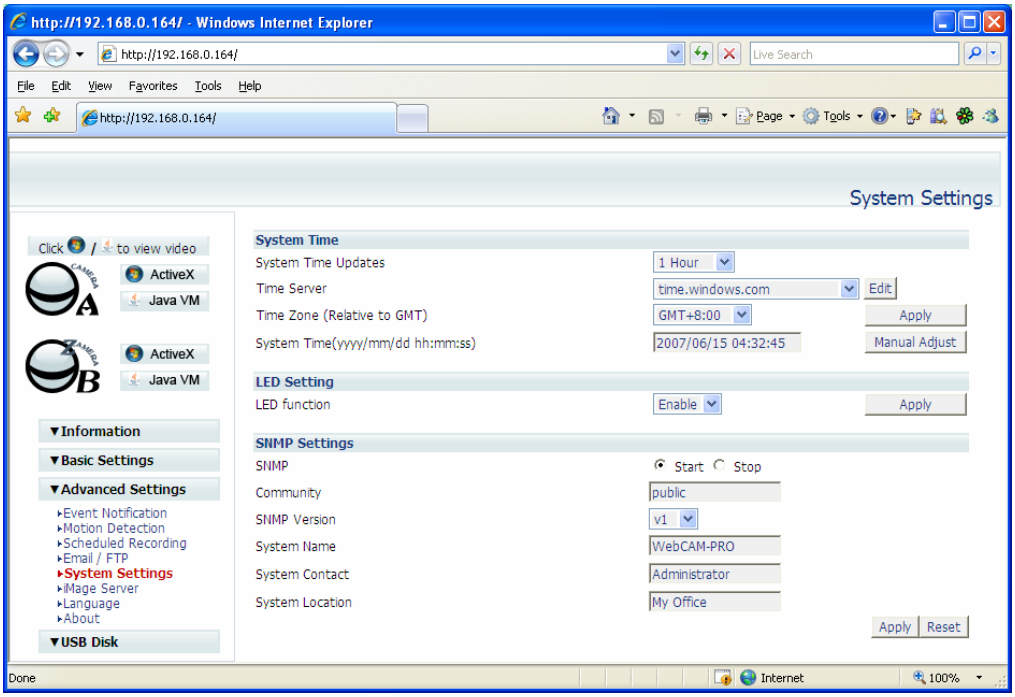


Fig.48 System Setting

i. System Time

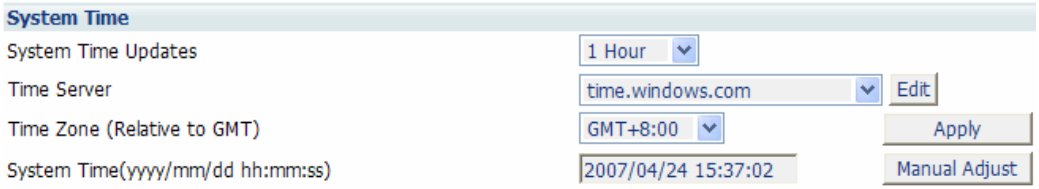


Fig.49 System Time

“System Time Updates”

You can set an interval for time synchronization. Select either 1, 3, 12 hours or 1, 10 & 30 days.

“Time Server”

Choose the nearest Time Server to your iGuard location. You can choose from the list of a maximum of 30 Time Servers.

To add a new Timer Server you must first make space by deleting some Time Servers. Once this is done, the add dialog box will appear as below. Click “Back” to return to the System Settings Page.

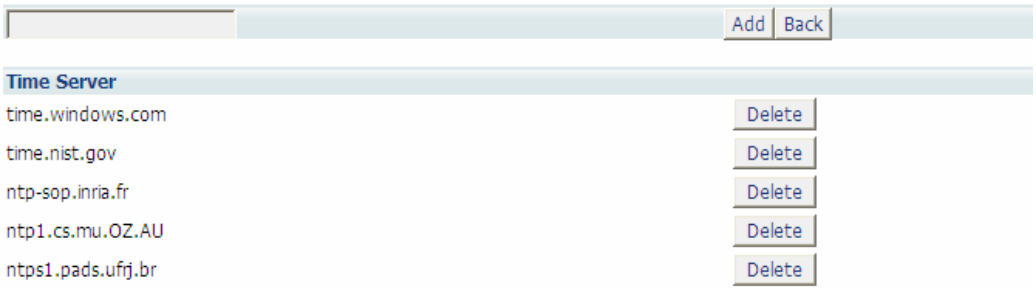


Fig.50 List of Time Server

“Time Zone (Relative to GMT)”

Select the appropriate time zone for your area. Click **“Apply”** to save.

“System Time (yyyy/mm/dd hh:mm:ss)”

This is to manually set iGuard System Time. The format is pre-determined to: yyyy/mm/dd hh:mm:ss. Click **“Manual Adjust”** to save any manual changes.

Note:
The camera has to be connected to the internet to have its time updated by the time server. The camera will not retain its clock setting if power is lost.

ii. LED Settings



Fig.51 LED Settings

LED function

If disabled, the Blue LED which indicate if a remote user is logged on and viewing the camera will not light.

iii. System Restart

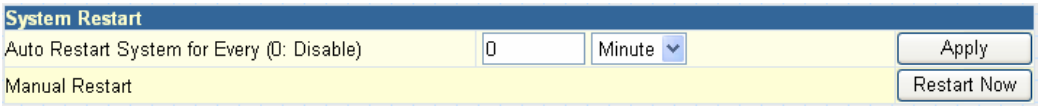


Fig.52 Auto Restart setting

“Auto Restart System Every”

You can choose to restart iGuard at certain intervals (choose between minutes and hours only). This will ensure that iGuard will work smoothly. Click “Apply” to save changes.

“Manual Restart”

Click “Restart Now” to restart the system immediately.

iv. SNMP Settings



Fig.53 SNMP setting

SNMP

Choose to enable or disable this feature.

Community

Assign a unique Community name for this unit that is identifiable in a Network Management System (NMS).

SNMP Version

Select the SNMP version supported by the system.

System Name

This is to give iGuard a name identifiable in a SNMP network.

System Contact

This is to give the Administrator an identity in the SNMP network.

"System Location"

This is to set iGuard location.

5. 2.4.6 About

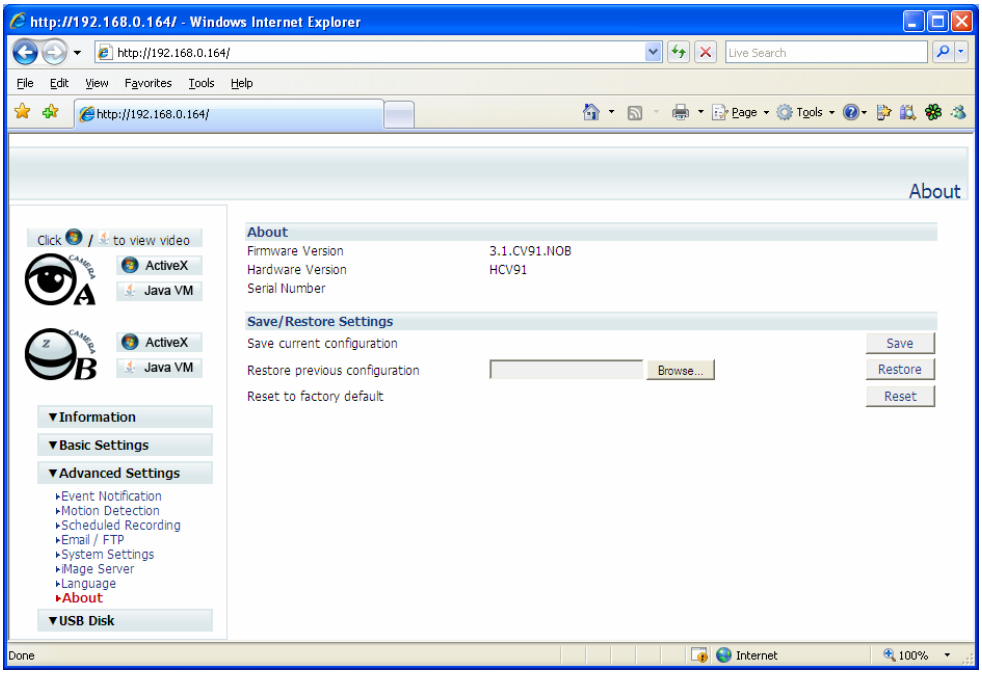


Fig.54 iGuard About Page

You can use this to check firmware information, save/restore settings, upgrade firmware and see manufacturer's details.

i. About

This gives crucial information about iGuard's Firmware Version, Hardware Version and Serial Number. These are required information for service calls.

ii. Save / Restore Settings

"Save current Configuration"

Click "Save" to save the current settings and configuration to your PC. The text file will have a default format of YYYY_MMDD_####.cfg. You can change this, if necessary.

"Restore previous configuration"

This function is only available if a setting has been saved initially. Browse to the location where the file is saved and click "Restore"

"Reset to factory default"

This function will reset all settings to its default value.

5.2.5 USB Disk

One of the unique features of the iGuard system is its ability to store video or images on a local drive through the USB expansion port, be it an iPod, a USB thumb drive or an External USB hard drive. The images are stored on a daily basis.

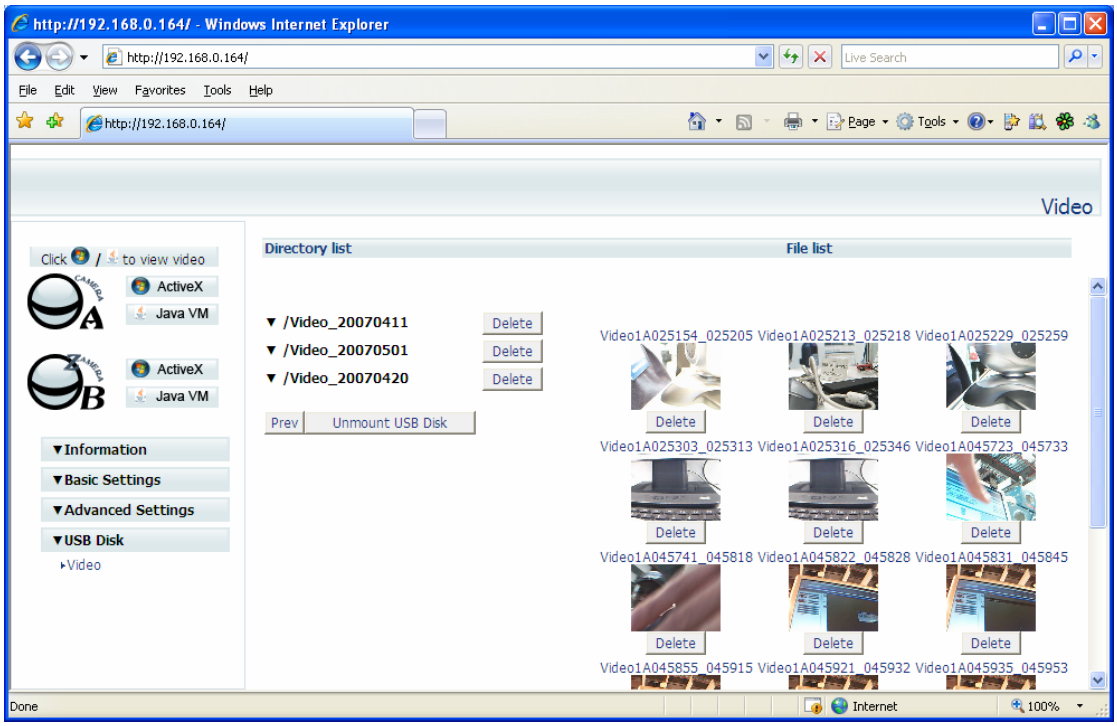


Fig.55 iGuard DVR

Note:
This section is only available if a USB flash disk with FAT32 format is connect. Administrator privilege is required to configure this section. You have to dismount the drive before removing it from the camera.

i. Directory List

Click the directory to display the content. All videos will be shown with a preview. You can select one or all video clips by checking on the selection box.

ii. Playback the video

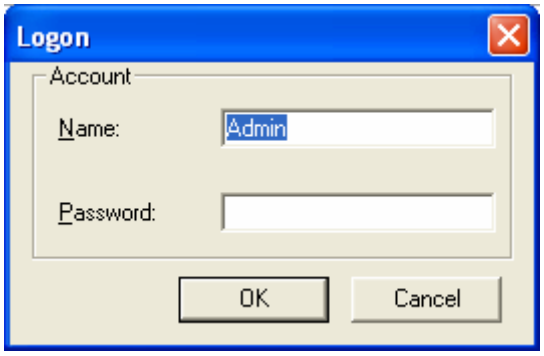
Click on the video to download it to your PC. Your default media player will be automatically launched to play the file.

Chapter 6: iGuardView

iGuardView is a PC based software that allow you to manage, monitor, and record multiple iGuard cameras located either in a LAN or on a WAN, or a combination of both

You can launch the iGuardView program by clicking on “start”/“All Programs”/ “iGuard” / “iGuardView” on your desktop.

The following Login window will be displayed.



By default, the Account Name is set to **“Admin**” and No Password

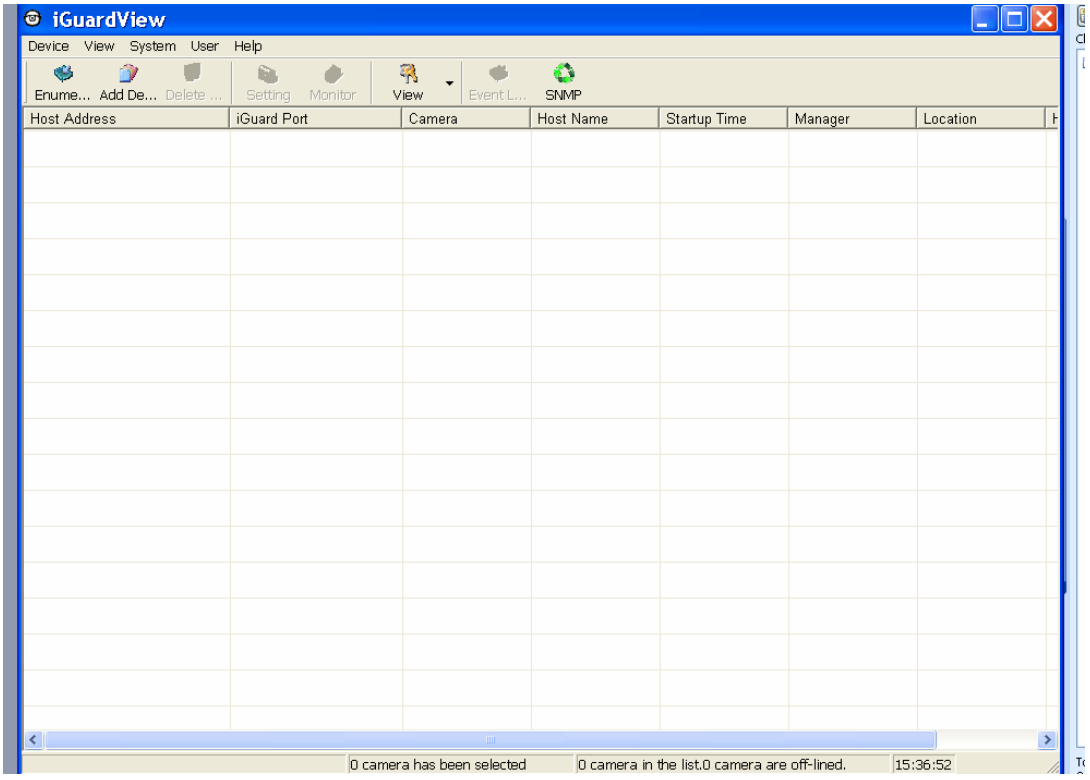


Fig.56 iGuardView Screen Shot

6.1 Adding Cameras



: Press the “Enumerate” button, iGuardView will start searching for all iGuard cameras under the same subnet and list them in the main window.

Once detected, the following will show in the main window:

Host Address	iCAMView Port	Camera	Host Name	Startup Time	Manager	Location
192.168.0.30	9001	Camera A				

This shows that the camera is online and active.

Host Address	iCAMView Port	Camera	Host Name	Startup Time	Manager	Location
192.168.0.30	9001	Camera A				

This shows that the camera is off-line



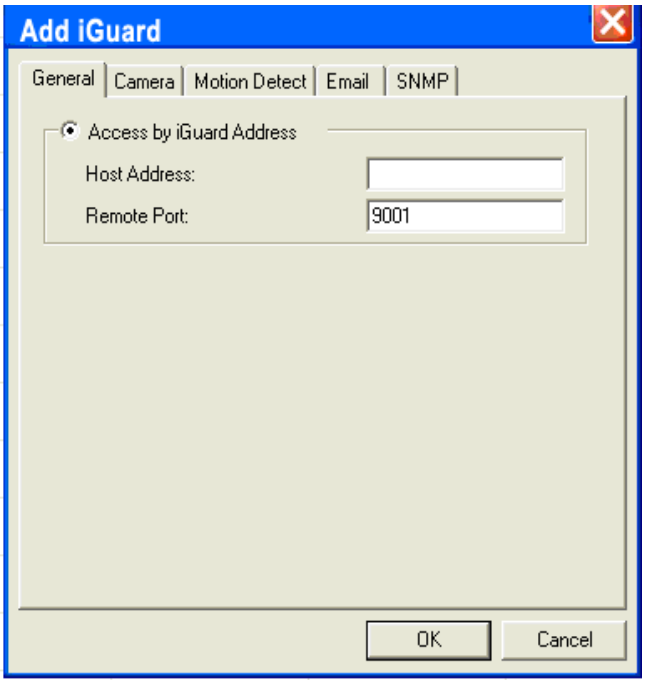
You can manually add any remote iGuard cameras to the list for monitoring

“Access by iGuard Address”

Enter the IP address of the iGuard (example: 192.168.0.30)

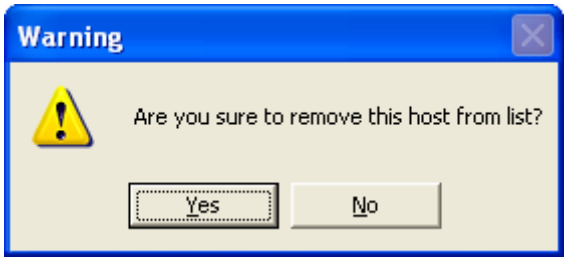
“Remote Port”

This is iGuard UDP port.





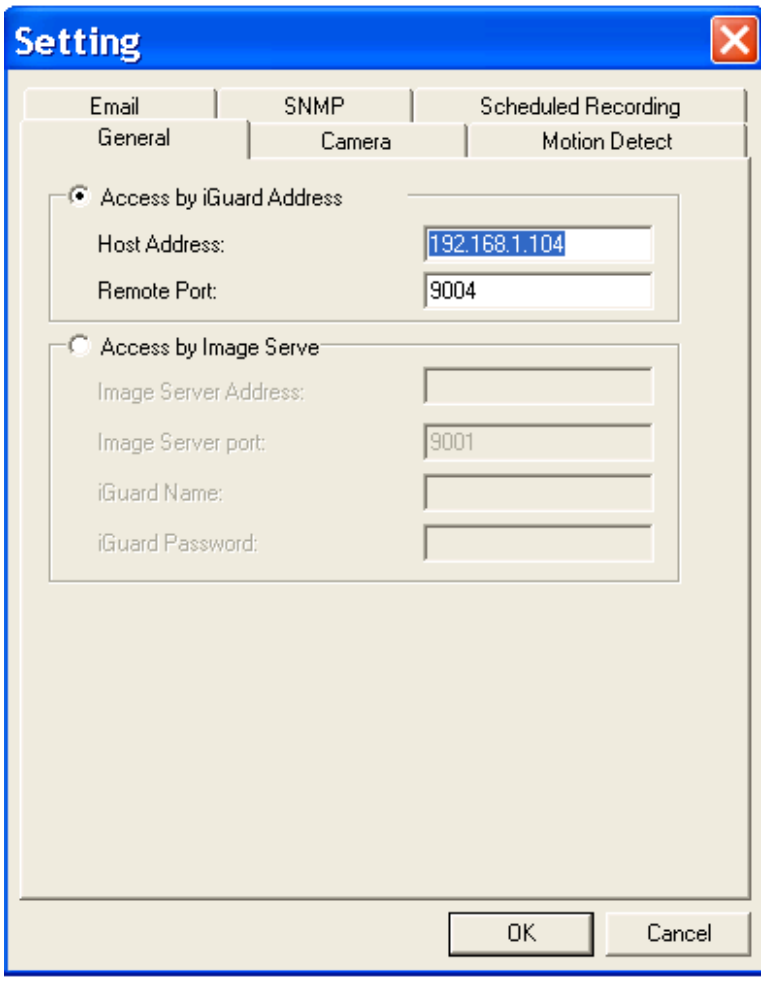
Highlight the iGuard to be deleted from iGuardView's list. Click : "Yes" to confirm deletion of selected iGuard.





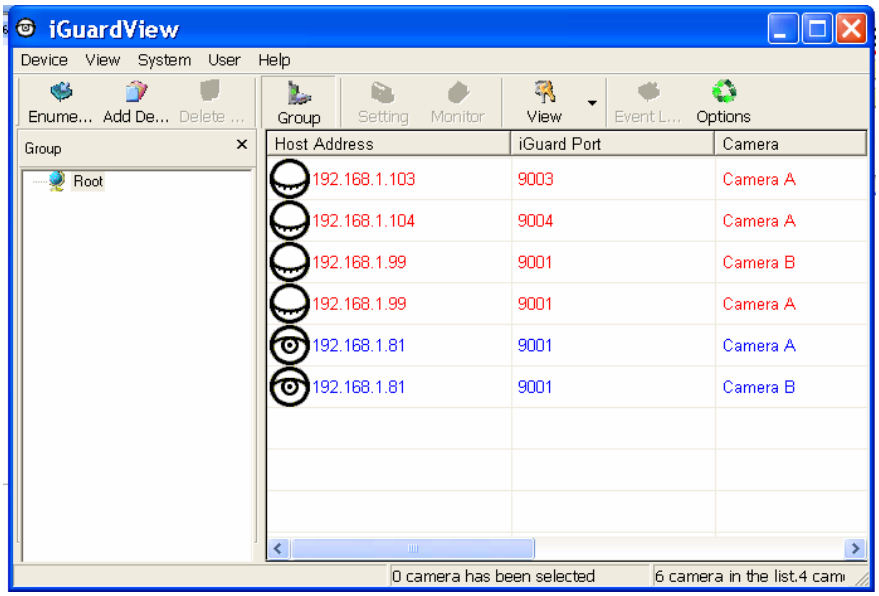
:

Use this function to change iGuard Address & Port Number.





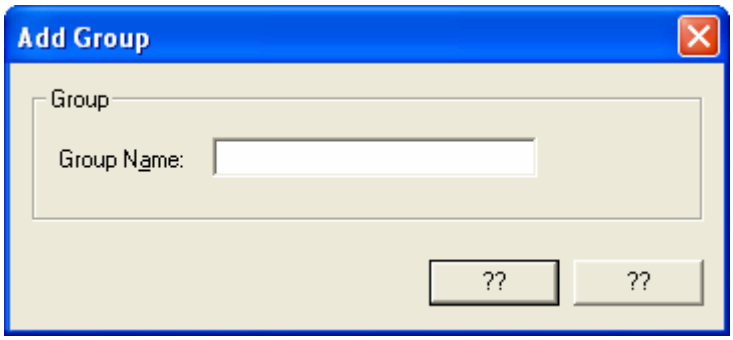
You can organize the cameras into groups for easy viewing.



Right click on the **Root** icon to bring up the option box.

Add group…

Click to bring up the add group window. Assign a name to the group. Sub-groups can be created using the same process.



Delete group

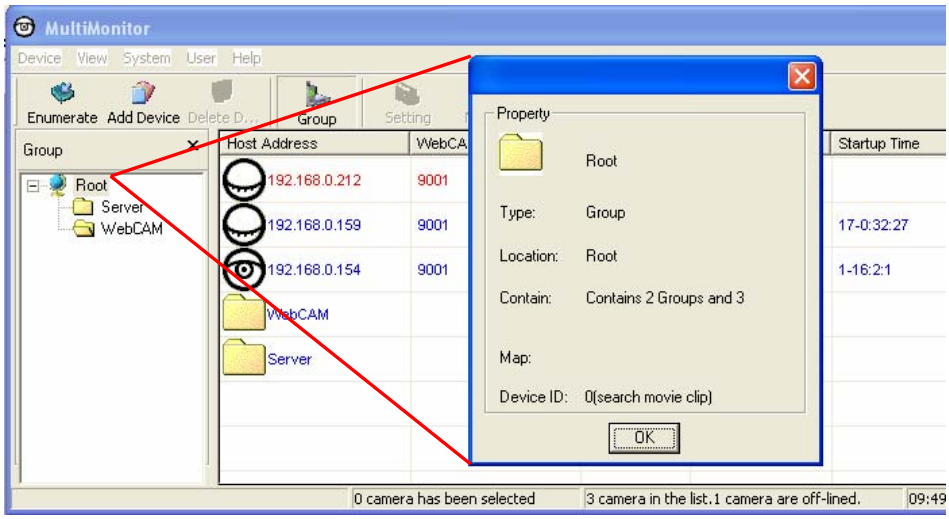
Click to delete the highlighted group.

Rename

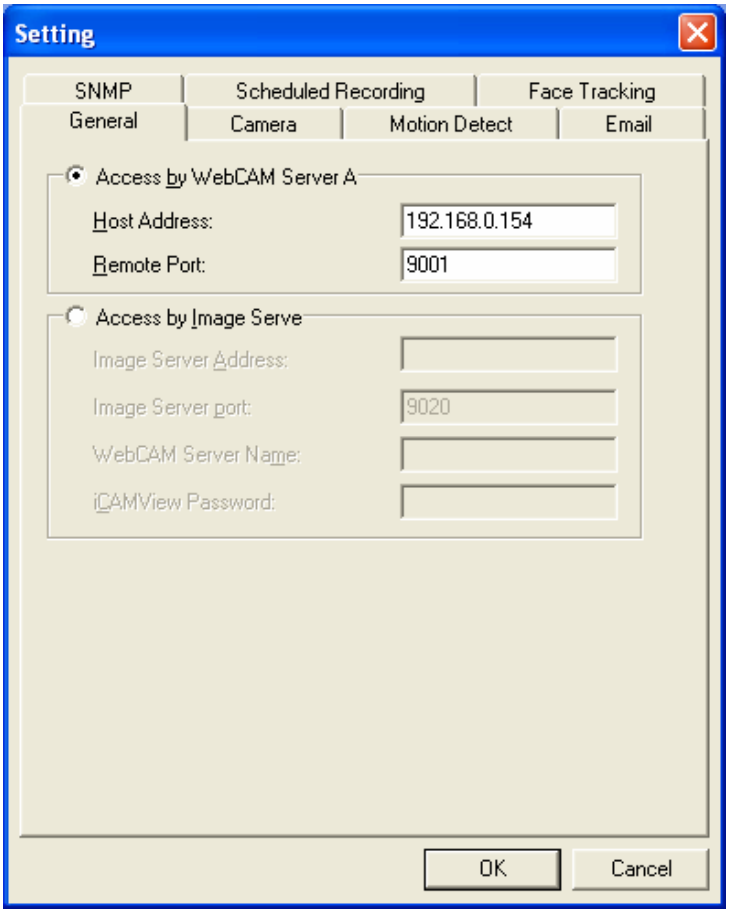
Click to rename the group.

Properties…

Click to bring up the group properties dialog box.



6.2 Camera Setting



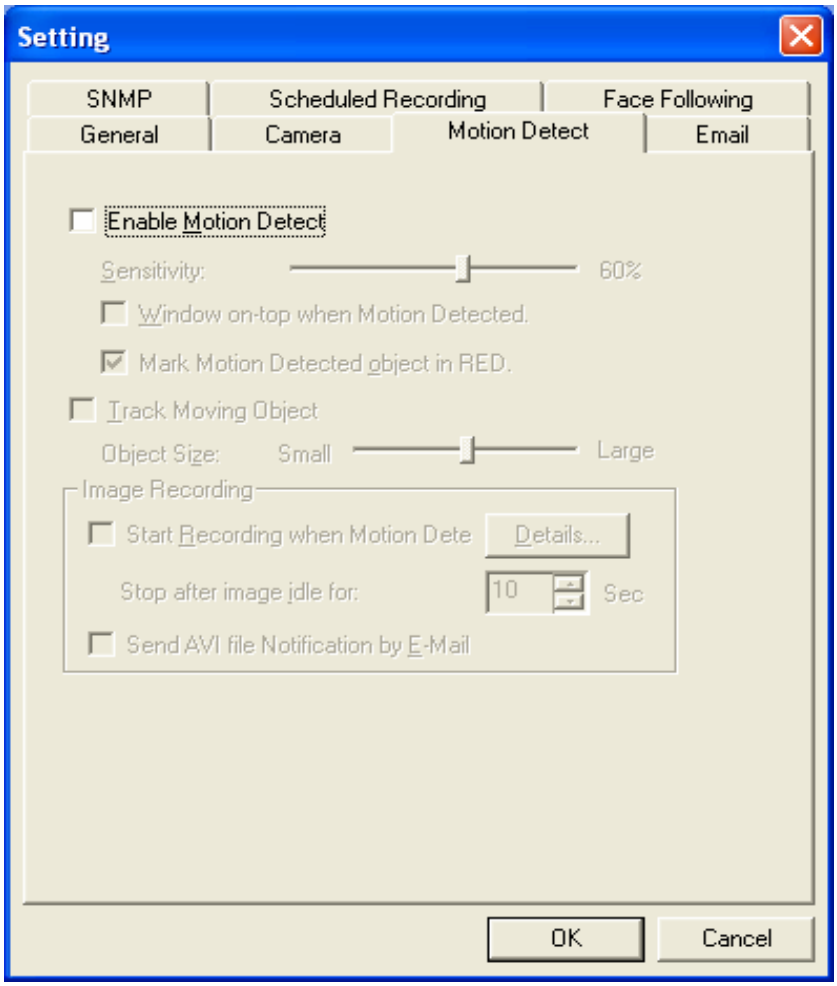
Camera Select: Select either camera A or B

Account: If you have setup user account, the information must be entered here. Otherwise access will be denied.

Password: Enter the above account password.

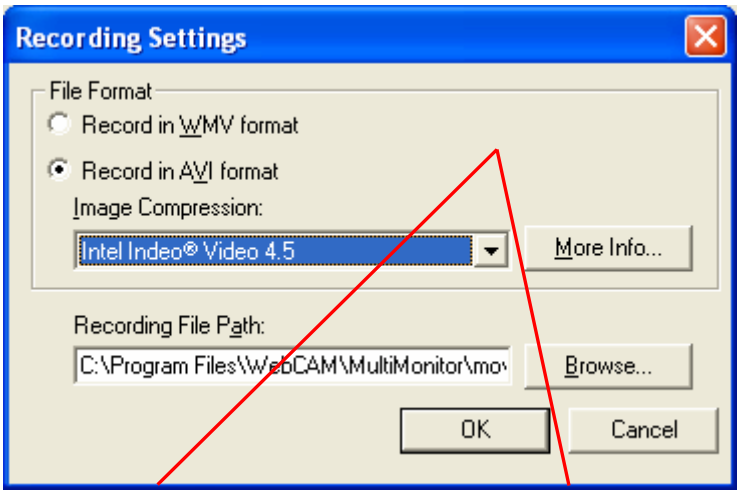
Image Zoom:	Resize the window to between 25% and 200%
Camera Rotation:	Use this function to keep the camera up-right.
Mirror the Image:	To mirror the image.
Maximum frame per second:	Select from 0.01 fps to a maximum of 30.00 fps. Default is set to 10.00 FPS.

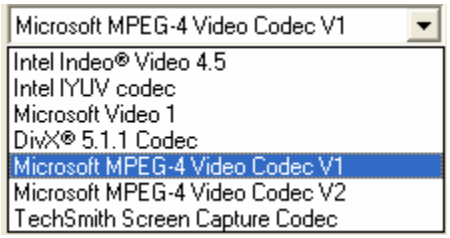
6.3 Motion Detection Setting



Enable Motion Detection:	Click the checkbox to enable Motion Detection. **Note:** This feature does not require the Camera Window be active to work.
Sensitivity:	Choose from 0% to 100% (very sensitive)

Window on-top when Motion Detected	Automatically displays camera window on top of all other windows/applications when motion is detected.
Mark Motion Detected object in RED	Choose this option to highlight in RED which object is being tracked.
Motion Tracking	Enabled this function to allow PTZ cameras to follow moving objects.





File Format	Choose between WMV or AVI format. For AVI select additional option under **Image Compression.**
Image Compression:	Choose from the list for available Codec in your PC. **Note:** This list is dependent on the Codec that is already installed on the local PC. To record in MPEG-4, make sure you install or upgrade to Windows Media Player v10.

Recording AVI File Path

Note:

a. Recorded files are saved using the following file extension;

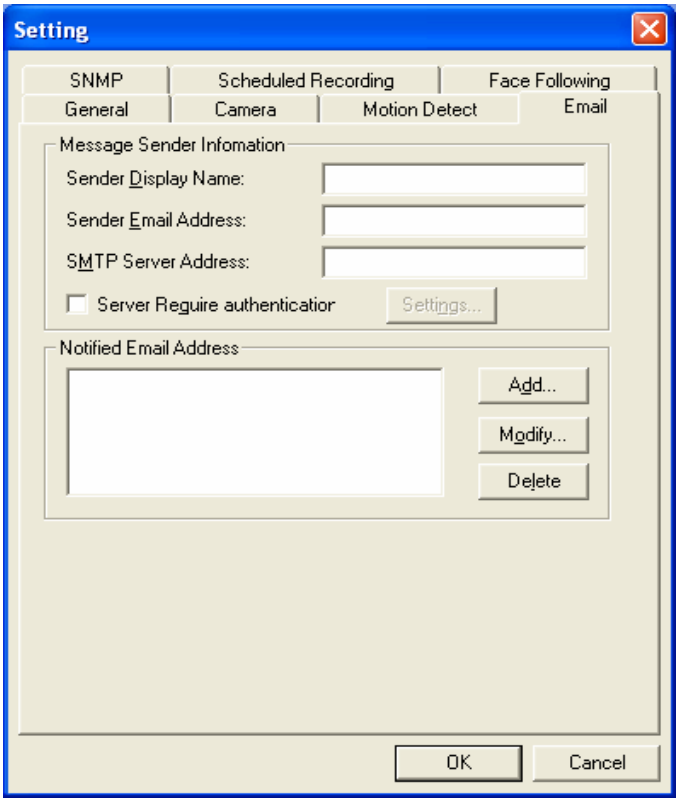
avifile[three digit numerical sequence].

b. Use the **Detail View** to check the stop time. You can change the display view or add a new folder here.

Stop after idle for:	Set the value between 1 to 100 seconds

Send AVI file Notification by Email:	Send an AVI file via email in the event any motion is detected.

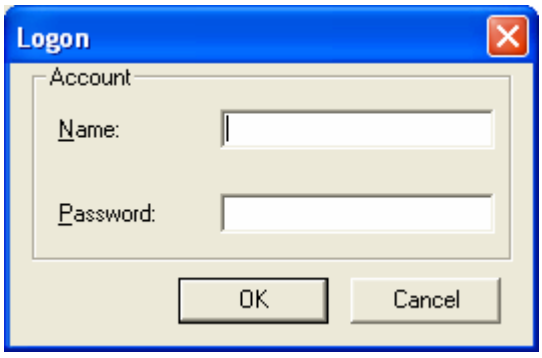
6.4 Email Notification Setting



You will need to configure the “Message Sender Information” in order for iGuardview to send emails.

Server Authentication

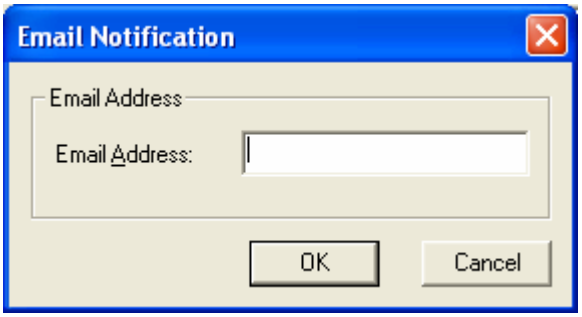
Click “settings…”



Enter your Account Name and Account Password if your Server Requires Authentication.

Email Address

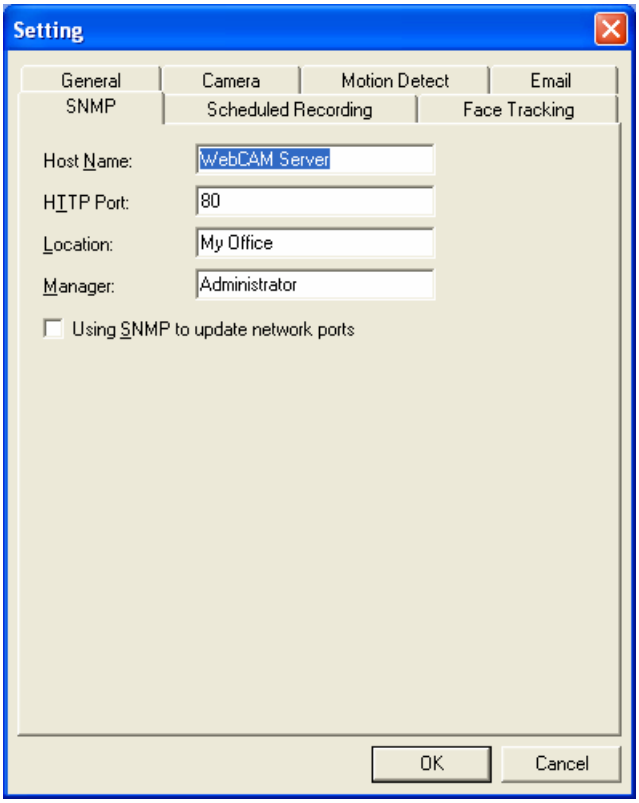
Click “Add…” and enter a new Email address below



Click **Modify…** to modify the entered Email Address

Click **Delete** to remove an email address from the notification list.

6.5 SNMP Setting



Host Name: Provide a Name to identify this device.

HTTP Port: Enter the HTTP port assigned for iGuard. Default is **80**, or check in the Web Interface under **Basic Settings → Networks → Port Number**.

Location: Provide a location for administrator to track device.

Manager: Enter an administrator's name for identification.

Use SNMP to update network ports

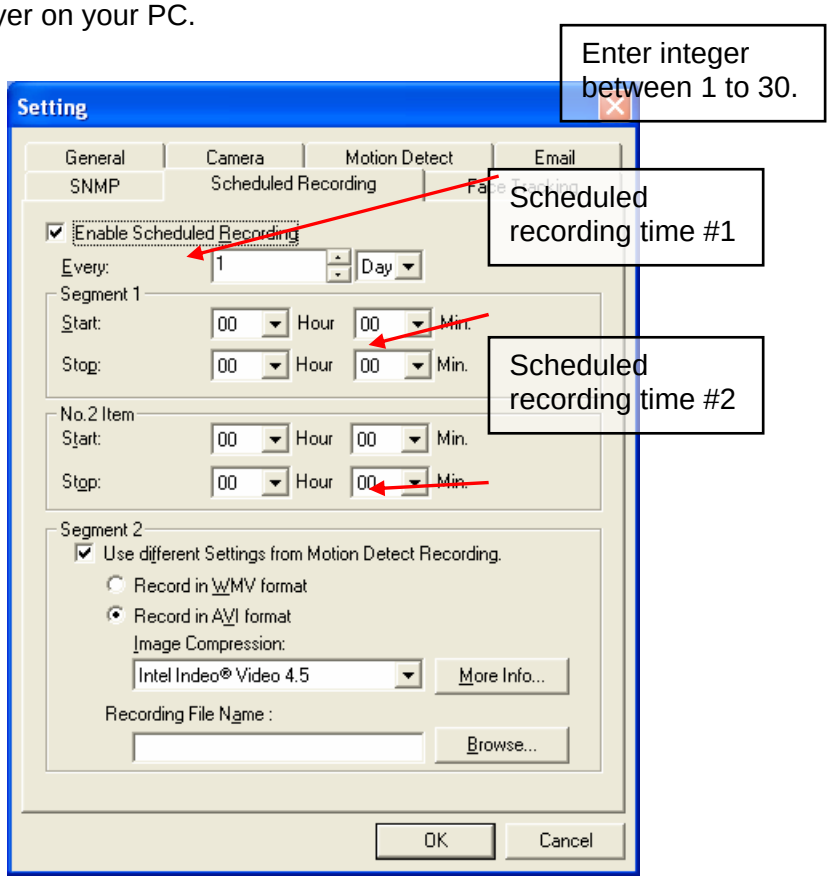
Check this box if you want iGuardView to automatically update the HTTP port as

set in;

a. Web Interface, **Basic Settings → Network → Port Number → HTTP port number** *or* in
b. Utility, **IP Configuration → Advanced → Management Protocol**

6.6 Schedule Recording

You can perform scheduled recording on iGuard. For 24 hour recording, you can set the following: Start: 00:00 End:23:59. The recorded files will be recorded in the designated folder on weekly basis with the folder named as the date of the Sunday for the week. Highlight and double click the recorded file to playback the video in the default media player on your PC.



6.7 Camera Monitor



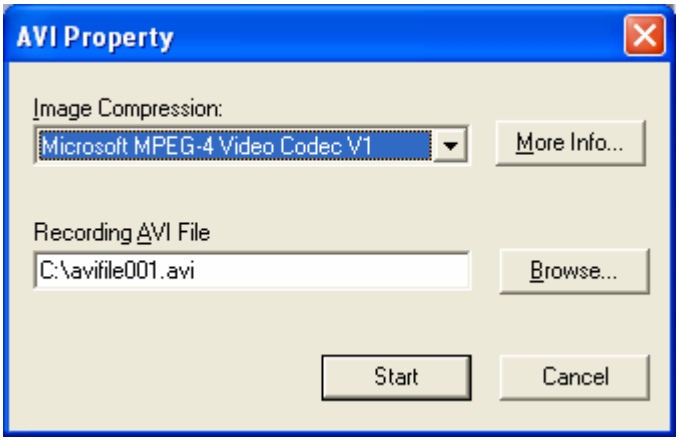
: Highlight the iGuard in the main windows display, and click “Monitor” to view the video stream.



Move the curser over the edges of the picture and it will turn into an arrow. Click and hold to pan / tilt the camera (if the camera supports this function)



Click this button to record the current image on screen. A window will come up, click “Start” to start recording to the default file and location.





Flip the image vertically



Rotate Left, Rotate Right



Click this to bring up the Setting windows.



Click this to switch to full screen view. Double click to switch back to current view.



Click and drag to resize the window and it’s contents.



Date and Time display of live streaming video.



Click the left side of the viewing window to bring out more control features.



Click on this icon to active two functions;

a. Custom window zoom – use this to zoom to your chosen window size.

On the video window, **LEFT** click, hold and drag to the desired window zoom size. A thin line will outline the chosen window size.



Release to accept and the program will auto adjust. Increase the Resolution for a better image.



Click the depressed  button to go back to the original window size.

b. Custom update Window -- use this if you want to monitor only a specific area within the viewing window.

On the video window, **RIGHT** click, hold and drag to the desired window zoom size. A thin line will outline the chosen window size.



Release and a smaller window is shown. Video in this smaller window will be updated while those outside are 'frozen'.

Click the depressed  button to go back to the original window size. Or use the horizontal zoom bar (see below).



Click and drag the green knob along the horizontal bar to zoom in an out. Zoom range from 1 time to 16 times.

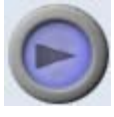


Click and drag the green knob along the horizontal bar to change the current image resolution. Resolution range from 320x240 low/mid/high quality, to 640x480 low/mid/high quality.



Clicking once will cause the camera to pan left by 1 deg.

Click and hold and the camera will pan increasingly faster to the left.



Clicking once will cause the camera to pan right by 1 deg.

Click and hold and the camera will pan increasingly faster to the left.



Click once to tilt the camera up by 1 deg.

Click and hold and the camera will tilt increasingly faster upwards.



Click once to tilt the camera down by 1 deg.

Click and hold and the camera will tilt increasingly faster downwards.



Auto Pan (if camera which support this function)

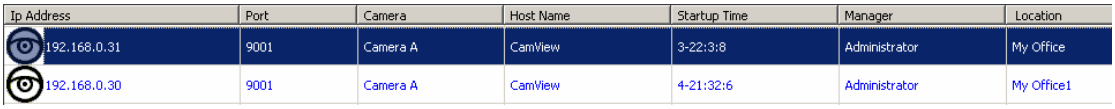
6.8 MuiltiView



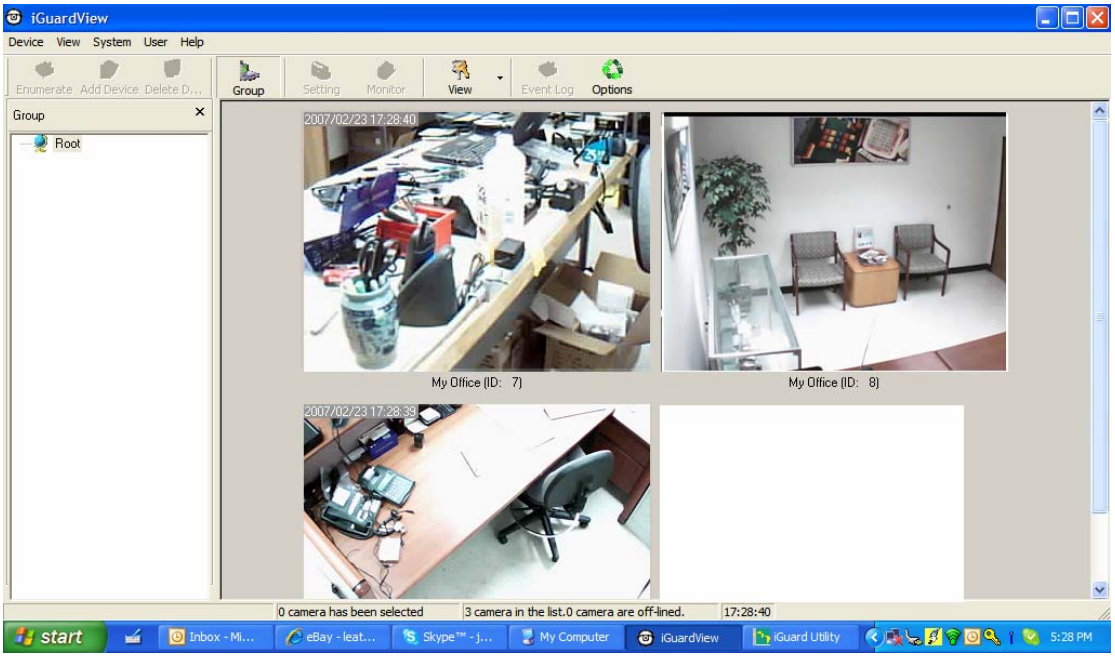
: Switch between Large or Small icon view or multi-view



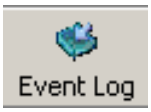
Large icon display



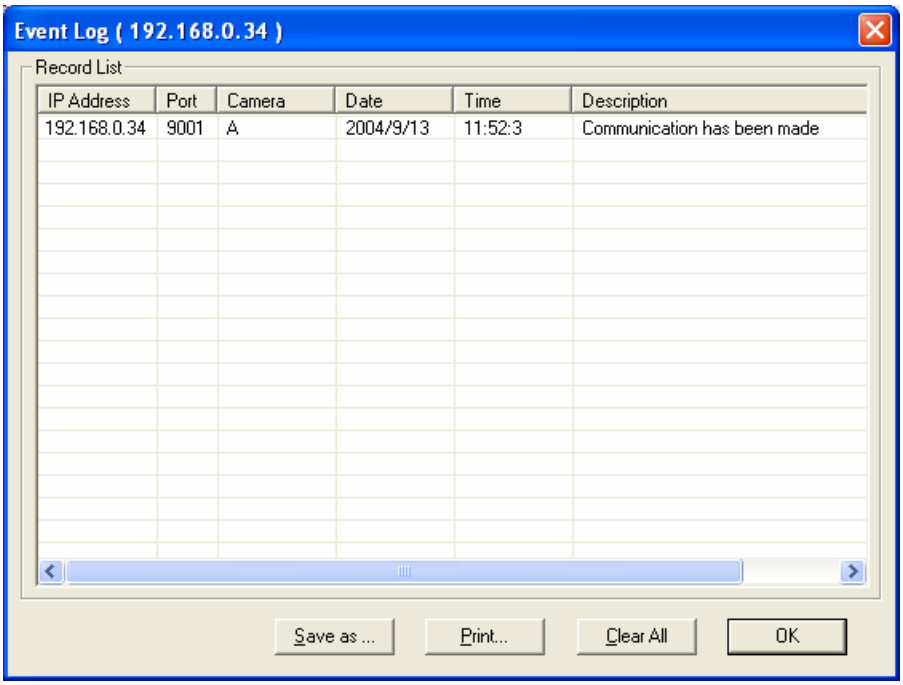
Small icon display



6.9 System

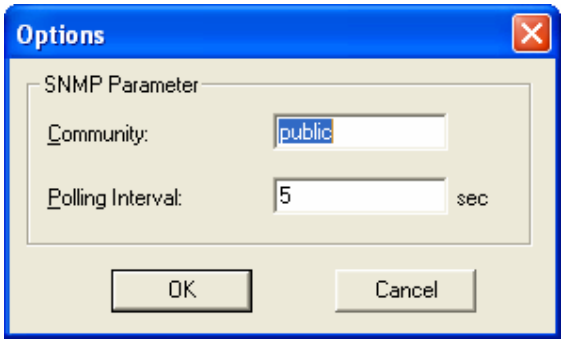


: Display the Event Log (IP address, Port, date, Time, description of event) of the selected iGuard.



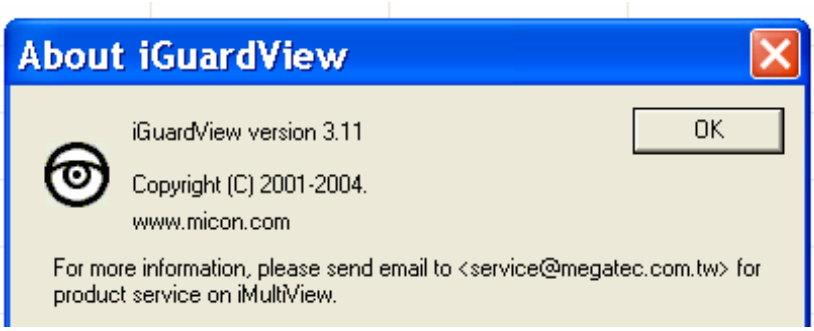


: Set the SNMP Parameter.



6.10 Help

Help : Display iGuardView version, Copyright information and product service contact.



Chapter 7: iGuard Mobile

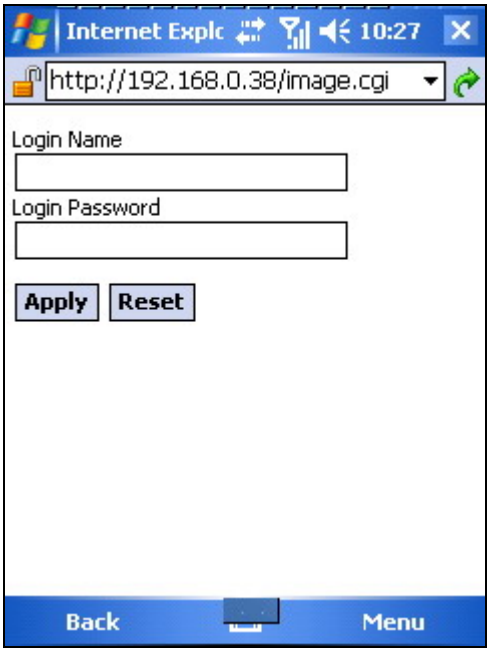
Currently iGuard supports static image viewing from a GRPS / WiFi enabled PDA / PPC / Symbian mobile device. A java based mobile video monitoring application for Windows Mobile devices is being developed please check our website for launch date.

To view the static images;

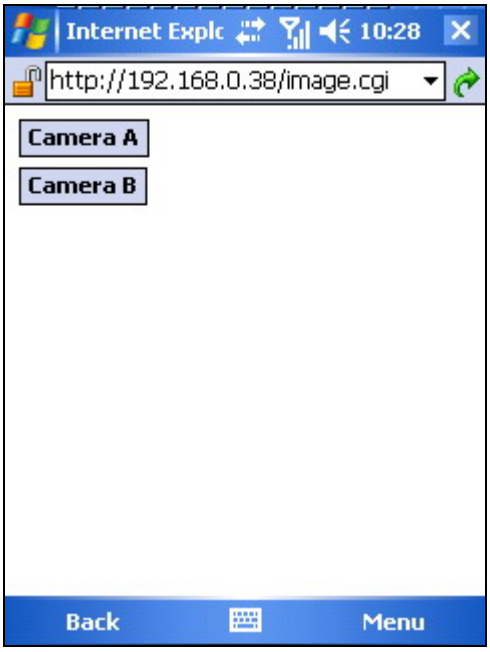
a. Make sure that the PDA / PPC / Mobile unit is connected to the Web.

b. Enter **http://xxx.xxx.xxx.xxx/image.cgi** in the web address (where **xxx** is either the LAN IP, WAN IP address or IGuard Domain Name)

c. The following login page will appear. Enter the **Login Name** and **Login Password** if applicable. Otherwise, click **Apply** to proceed.

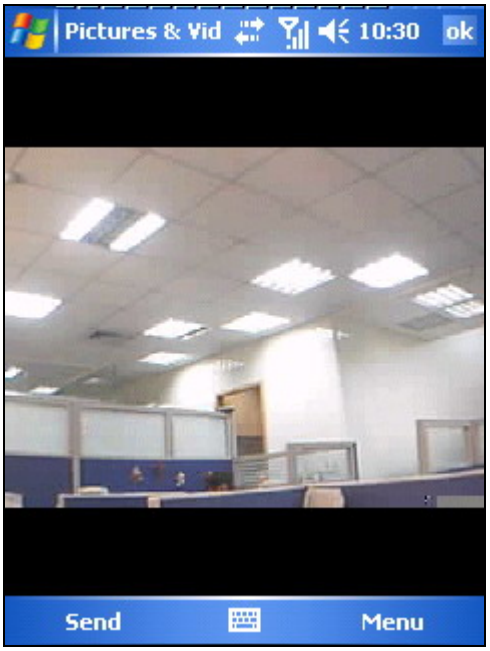


d. The following Camera Selection will appear. Click on either **Camera A** or **Camera B**.



e. The default file name is **showimg_pda.jpg**, click **Save As…** to change the file name or save location.





Note:
The downloaded image size depends on the resolution set in **Basic Settings → Camera Settings → Image Size**.

Approximately; 6KB @ 320x240 vs. 17KB @ 640x480 resolution.

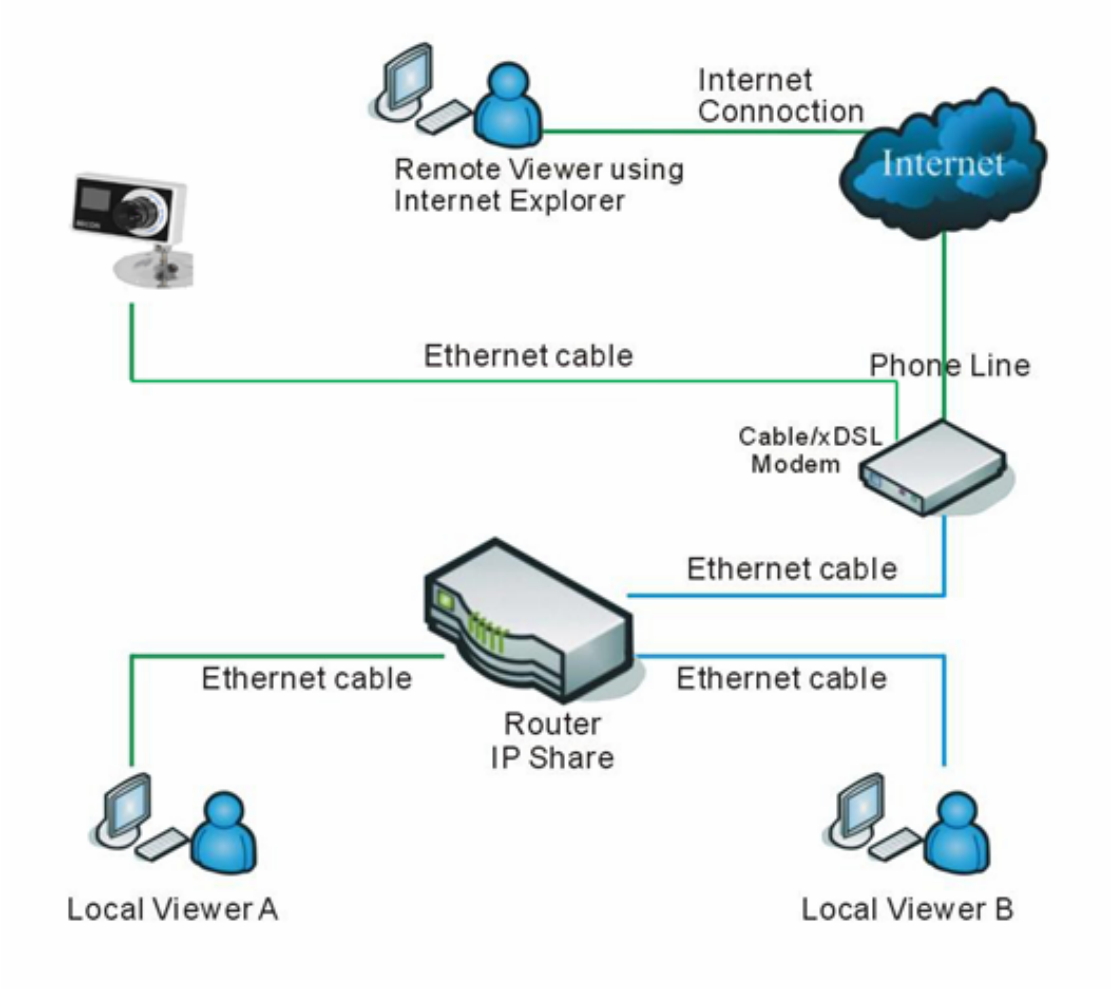
f. The images are downloaded and displayed one at a time. Click **Refresh** to download the next image. Click **Back** to go to the camera page to select a different camera.


Internet Explc
11:03
http://192.168.0.38/select_ima
Refresh Back
Back
Menu

Appendix A: Network Configuration /Router Programming

A.1 Static IP address

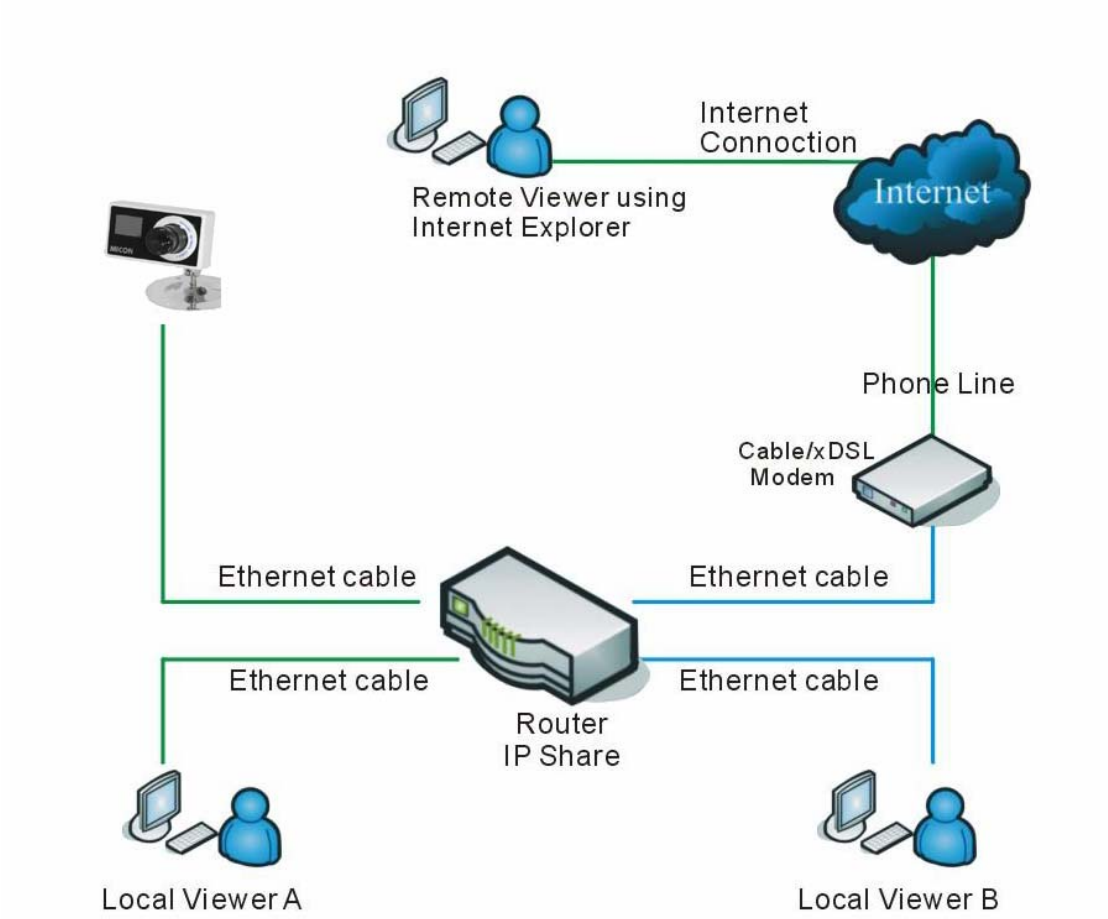
Most Internet service provider (ISP) offer some type of commercial grade service which will assign one or more static public IP addresses to your organization. If you allocate one of these static public IP address to the iGuard, then without further programming, you can monitor the camera on line from anywhere in the world, given the camera is connected to the cable/DSL modem directly.



A.2 Dynamic IP Address

If you have signed up a consumer grade broadband service with a dynamic IP address, or you use a router to share your internet access you will need to address one or all of the following issues:

a. DDNS service
b. Port forwarding
c. Firewall



a. DDNS:

In order to access the iGuard from internet, you will have to know the external IP address of your router. If you have a consumer grade broadband service, this IP address may change over time, making it impossible for the remote PC to communicate with your iGuard, just like you ask people to call you but you change your phone number without notified the other party. As value added service, iGuard.com hosts a DDNS server that tracks iGuard's IP address for this very reason reason. Please logon to www.iguard.com for more info.

b. Port Forwarding

If you place the iGuard behind a router, you need to programme the router so that it can direct the specific incoming traffic to iGuard, exactly in the same fashion how the telephone switch in your office works.

By default iGuard uses Port 80 for HTTP traffic (web manager) and port 9001 for video streaming. So you need forward port 80 traffic to the internal IP address of the iGuard.

If your Internet service Provider blocks port 80, which is quite common for DSL providers, or you already host a website on the same network, you'll need to reconfigure your iGuard and router to use different ports such as 81/9002, 82/9003, etc.

For multiple camera installation, each iGuard has to be assigned a unique IP address and port number.

Note: The section you need to look for in the router is Port Forwarding or Virtual Server

C. Firewall

iGuard uses port 9001 by default to stream video to the internet. Unfortunately this port is normally disabled or blocked by most commercial router's firewall or the built-in firewall utility on Windows XP. In order for the iGuard applications to work properly, the firewall settings in the router need to be configured.

Some router has a very sophisticated built-in firewall. Instead of programming each port on the router, you can use the DMZ feature to by-pass the firewall setting.

Follow the steps below to configure your router. If your particular router manufacturer or model is not listed below, please contact your router manufacturer for further assistance in configuring the router, or visiting www.portforwarding.com for more information.

Router Programming

The Following Router manufacturers and models are included in this document:

Brand	Model	Description
3Com	3C857-US	OfficeConnect Cable/DSL Gateway
	3CRWE52196	OfficeConnect Wireless Cable/DSL Gateway
Belkin	F5D6230-3	Wireless Cable/DSL Gateway Router
	F5D7230-4– 54g	Wireless DSL/Cable gateway Router
D-Link	DI-604/DI–614+/DI-624	-
	DI-704/704P	-
	DI714	-
	DI-714P+	-
Dell	TrueMobile 2300 Wireless Broadband Router	-
Linksys	BEFSR41	EtherFast Cable/DSL Router
	BEFSX41	Instant Broadband EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN EndPoint
	BEFW11S4	Wireless Access Point Router with 4-Port Switch – Version 2
Microsoft	MN-100	Wired Base Station
	MN-500	Wireless Base Station
NETGEAR	RP614	Web Safe Router
	MR814	Wireless Router
	MR314	Cable/DSL Wireless Router
	FVS318	ProSafe VPN Firewall

Proxim	ORiNOCO BG-2000 Broadband Gateway	-
Siemens	SpeedStream 2602	2-Port DSL/Cable Router
	SpeedStream 2623	Wireless DSL/Cable Router
	SpeedStream 2604	4-port DSL/Cable Router
	SpeedStream 2624	Wireless DSL/Cable Router
SMC	SMC2404WBR	Barricada Turbo 11/22 Mbps Wireless Cable/DSL Broadband Router
	SMC7004VBR	Barricada Cable/DSL Broadband Router
	SMC7004CWBR	Barricada Wireless Cable/DSL Broadband Router
	SMC7004AWBR	Barricade 4-port 11Mbps Wireless Broadband Router

3Com (http://www.3com.com)

3C857-US – OfficeConnect Cable/DSL Gateway
3CRWE52196 – OfficeConnect Wireless Cable/DSL Gateway

1. Log into your router using your router IP.

2. On the main page, select **Firewalls** on the left side of the page.

3. Select the **Virtual Servers** tab at the top of the page.

4. Click **New** on the right side of the page to open the Virtual Server Settings dialog box.

5. Type in the camera's IP address in the Server IP address text box. (Look on the iGuard IP address LCD display for the last 3 digits of the camera's IP address.)

6. Under Local Service, select **Custom**.

7. Under Custom Service Name, type in: **iGuard**.

8. Under Specify Custom Service Ports, type in: **80, 9001**.

9. Click **Add** to save the settings. The iGuard should now be configured to work with your router and be accessible from the internet.

Belkin (http://www.belkin.com)

F5D6230-3 – Wireless Cable/DSL Gateway Router

1. Log into your router using your router IP.

2. On the main page, select **Virtual Server** on the left side of the page under the Securit section.

3. Enter the following information on the page:

Line #1:

Private IP:	Type in the **camera's IP address**. (Look on the iGuard IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	80
Type:	TCP
Public Port:	80

Line #2

Private IP:	Type in the **camera's IP address**. (Look on the iGuard IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	9001
Type:	UDP
Public Port:	9001

4. Click **Enter** to save the settings. The iGuard should now be configured to work with your router and be accessible from the internet.

F5D7230-4 – 54g Wireless DSL/Cable gateway Router

1. Log into your router using your router IP.

2. On the main page, select **Firewall** on the left side of the page.

3. Under Firewall, select **Virtual Servers**.

4. Enter the following information on the page:

Line #1

Enable:	Checked in
Description:	iGuard - Webpage
Internet Port:	80 to 80
Type:	TCP
Private IP address:	Type in the **camera's IP address**. (Look on the iGuard Address LCD display for the last 3 digits of the camera's IP address)

Private Port	80 to 80

Line #2	
Enable:	Checked in
Description:	iGuard – Camera
Internet Port:	9001 to 9001
Type:	UDP
Private IP address:	Type in the **camera's IP address**. (Look on the iGuard Address LCD display for the last 3 digits of the camera's IP address)
Private Port	9001 to 9001

5. Click **Apply Changes** to save the settings. The iGuard should now be configured o work with your router and be accessible from the internet.

D-Link (http://www.dlink.com)

DI-604/DI – 614+/DI-624

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the left side of the page, click on **Virtual Server**. Note: Make sure DMZ host is disabled. If DMZ is enabled, it will disable all Virtual Server entries.

4. Enter the following information on the page:

Enable/Disable:	Enabled
Name:	iGuard - Webpage
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Protocol Type:	TCP
Private Port:	80
Public Port:	80
Schedule:	Always

5. Click **Apply** to save the settings.

6. Enter the following information on the page:

Enable/Disable:	Enabled
Name:	iGuard - Webpage
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Protocol Type:	UDP
Private Port:	9001
Public Port:	9001
Schedule:	Always

7. Click **Apply** o save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI-704/704P

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the **Virtual Server** page, enter the following information;

For ID#1:

Service Port:	80
Service IP:	Type in the **camera's IP address**, for example: 192.168.0.5

Enabled/Disabled: Enabled

For ID#2
Service Port: 9001
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

4. Save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI714

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. Click on **Virtual Server Settings** on the left side of the page.

4. Enter the camera's IP address into the Internal IP field. Under Service, select **All** and then click **Submit** to save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI-714P+

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the left side of the page, click **Virtual Server**.

4. Enter the following information on the page:
For ID#1:
Service Port: 80
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

For ID#2
Service Port: 9001
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

5. Click **Apply** to save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

Dell TrueMobile 2300 Wireless Broadband Router

(http://www.dell.com)

1. Log into your router using your router IP.

2. On the main page, click on **Advanced Settings** at the top of the page.

3. Go to the Port Forwarding and select Custom Port Forwarding Settings.

4. Check the **Enable** box.

5. Enter the desired name or description in the **Service Name** field such as **iGuard Web**.

6. In the **Incoming Ports** field, specify port **80** in both boxes.

7. In the **Destination IP Address** field, enter the IP address of iGuard

8. In the **Destination MAC Address** field, enter the MAC address of iGuard. You can find the camera's MAC address by either looking at the MAC address sticker on the bottom of the camera or by utilizing iGuard setup utility to display the MAC address.

Linksys (http://www.linksys.com)

BEFSR41 – EtherFast Cable/DSL Router

BEFSX41 – Instant Broadband EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN EndPoint

BEFW11S4 – Wireless Access Point Router with 4-Port Switch – Version 2

1. Log into your router using your router IP.

2. On the router's main page, click on **Advanced** at the top of the page.

3. On the next page, click on **Forwarding**.

4. Enter the following information on the page:

Line #1:

Customized Applications:	iGuard – Webpage
Ext. Port:	80 to 80
Protocol:	TCP
IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

Line #2:

Customized Applications:	iGuard – Camera
Ext. Port:	9001 to 9001
Protocol:	UDP
IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

5. Click on **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

Microsoft (http://www.microsoft.com/hardware/broadbandnetworking)

MN-100 – Wired Base Station
MN-500 – Wireless Base Station

1. Log into your router using your router IP.

2. Open the Bass Station Management Tool, and then click **Security**.

3. On the Security menu, click **Port Forwarding**, and then click **Set up persistent port forwarding**.

4. In the Enable checkbox, check in the checkbox.

5. In the Description box, type a description of the server field such as: **iGuard Web**.

6. In the Inbound port boxes, type in: **80 – 80**. (i.e. from Port 80 to Port 80)

7. In the Type box, select the protocol as **TCP**.

8. In the Private IP address box, type in the **IP Address** of the iGuard network camera. For example, type in: 192.168.0.5.

9. In the Private port boxes, these values are automatically filled in from Step 6 and should already show **80 – 80**.

10. On the next empty line, repeat steps 4-9, except this time the Description should be **iGuard Cam** and the Inbound/Private port boxes should be **9001 – 9001** (UDP). The protocol and private IP address should be the same.

11. Click **Apply** to save the changes you have made. iGuard should now be configured to work with your router and be accessible from the internet.

NETGEAR (http://www.netgear.com)

RP614 – Web Safe Router
MR814 – Wireless Router

1. Log into your router using your router IP.

2. Click **Advanced -> Port Forwarding** on the left side of the page.

3. Click Add Customer Service.

4. Enter the following information on the page:

Service Name:	iGuard – Web
Starting Port:	80
Ending Port:	80
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

5. Click **Apply** to save the settings.

6. Enter the following information on the page:

Service Name:	iGuard – Cam
Starting Port:	9001
Ending Port:	9001
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

7. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

MR314 – Cable/DSL Wireless Router

1. Log into your router using your router IP.

2. Click **Advanced** on the left side of the page.

3. Click **Ports**.

4. Enter the following information on the page:

Line #1:

Starting Port:	80
Ending Port:	80
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

Line #2:

Starting Port:	9001
Ending Port:	9001
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

5. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

FVS318 – ProSafe VPN Firewall

1. Log into your router using your router IP.

2. On the main page, click on **Add Service** on the left side of the screen.

3. Click Add Customer Service.

4. In the **Name** field enter a name for the camera, for example: **iGuard Web**:

Type:	TCP
Start Port:	81
Finish Port:	81

5. Click **Apply** to save the settings.

6. There is a bug in the NETGEAR FVS318 1.4 firmware that does not record any entry that uses port 80. If you intend to use port 80, you will initially need to enter 81 for the Start and Finish port, and then edit the entry to port back to 80. Click on **Add Service** on the left side of the screen.

7. In the **Service Table** window select iGuard Web and click **Edit Service**.

8. Change the **Start** and **Finish** port to **80**. Click **Apply**.

9. On the main page, click on **Add Service** on the left side of the screen and then click **Add Custom Service**. In the **Name** field enter a name for the camera, for example: **iGuard Cam**.

Type:	UDP
Start Port:	9001
Finish Port:	9001

10. Click **Apply** to save the settings.

11. On the main page, click on **Ports** at the side of the screen.

A. Click **Add**.

B. For Service Name select: iGuard Web

C. Action: **ALLOW always**

D. Local Server Address: Enter the IP address of the camera

E. WAN Users Address: **Any**

F. Click **Apply**.

12. Click Add again.

A. For Service name select: **iGuard Cam**

B. Action: ALLOW always

C. Local Server Address: Enter the IP address of the camera

D. WAN Users Address: **Any**

E. Click **Apply**.

13. Exit the router setup program. iGuard should now be configured to work with your router and be accessible from the internet.

Proxim (http://www.proxim.com)

ORiNOCO BG-2000 Broadband Gateway

1. Log into your router using your router IP.

2. On the router's main page, click on **Setup** at the top of the page.

3. On the left side of the page, click on **Advanced settings -> Port Forwarding**.

4. Check in the checkbox for **Enable Port Forwarding**.

5. Click **New** on the right side of the page.

6. Enter the following information on the page:

Global Port:	80
Local Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Local Port:	80
Type:	TCP

7. Click **Save** to save the settings.

8. Click **New** on the right side of the page.

9. Enter the following information on the page.

Global Port:	9001
Local Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Local Port:	9001
Type:	UDP

10. Click **Save** to save the settings.

11. Click **Restart** on the left side of the page to restart your router. iGuard should now be configured to work with your router and be accessible from the internet.

Siemens (http://www.speedstream.com)

SpeedStream 2602 – 2-Port DSL/Cable Router
SpeedStream 2623 – Wireless DSL/Cable Router
SpeedStream 2624 – Wireless DSL/Cable Router

1. Log into your router using your router IP.

2. After you are logged in, click on **Advanced Setup -> Virtual Servers**.

3. Enter the following information on the page:

Line #1:

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	80
Type:	TCP
Public Port:	80

Line #2

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	9001
Type:	UDP
Public Port:	9001

4. Click **Enter** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

SpeedStream 2604 – 4-port DSL/Cable Router

1. Log into your router using your router IP.

2. After you are logged in, click on **Advanced Setup -> Virtual Servers**.

3. Under the Properties section, there are a few entries you'll need to add. Check in the checkbox for **Enable**.

4. Under the first box, next to the Enable checkbox, type in: **iGuard Web**.

5. Under PC (Server), select your camera or the camera's IP address from the list. If the camera is not listed, select the link titled "My PC is not listed."

6. Leave Protocol as **TCP**.

7. Under Internal Port No type in: **80**

8. Under External Port No type in: **80**

9. Click on **Add** to save these settings.

10. Under the first box, next to the Enable checkbox, type in: **iGuard Cam**.

11. Under PC (Server), select your camera or the camera's IP address from the list. If the camera is not listed, select the link titled "My PC is not listed."

12. Leave Protocol as **TCP**.

13. Under Internal Port No type in: **9001**

14. Under External Port No type in: **9001**

15. Click on **Add** to save these settings. iGuard should now be configured to work with your router and be accessible from the Internet.

SMC (http://www.smc.com)

SMC2404WBR – Barricada Turbo 11/22 Mbps Wireless Cable/DSL Broadband Router
SMC7004VBR – Barricada Cable/DSL Broadband Router
SMC7004CWBR – Barricada Wireless Cable/DSL Broadband Router

1. Log into your router using your router IP.

2. After you are logged in, click **NAT** on the left side of the page.

3. Click on **Virtual Server** on the left side of the page.

4. Enter the following information on the page:

Line #1:

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	80
Type:	TCP
Public Port:	80

Line #2

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Private Port:	9001
Type:	UDP
Public Port:	9001

5. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the Internet.

SMC7004AWBR – Barricade 4-port 11Mbps Wireless Broadband Router

1. Log into your router using your router IP.

2. Click on **Virtual Server** on the left side of the page.

3. Enter the following information on the page:

For ID #1:

Service Port:	80
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Enable:	Checked in

For ID #2:	
Service Port:	9001
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5 (Look at iGuard's IP Address LCD display for the last 3 digits of the camera's IP address)
Enable:	Checked in

4. Click Save to save the settings. iGuard should now be configured to work with your router and be accessible from the Intern

Appendix B: IP Address, Subnet and Gateway

This section discusses Communities, Gateways, IP Addresses and Subnet masking

Communities
A community is a string of printable ASCII characters that identifies a user group with the same access privileges. For example, a common community name is "public." For security purposes, the SNMP agent validates requests before responding. The agent can be configured so that only trap managers that are members of a community can send requests and receive responses from a particular community. This prevents unauthorized managers from viewing or changing the configuration of a device.

Gateways
Gateway, also referred to as a router, is any computer with two or more network adapters connecting to different physical networks. Gateways allow for transmission of IP packets among networks on an Internet.

IP Addresses
Every device on an Internet must be assigned a unique IP (Internet Protocol) address. An IP address is a 32-bit value comprised of a network ID and a host ID. The network ID identifies the logical network to which a particular device belongs. The host ID identifies the particular device within the logical network. IP addresses distinguish devices on an Internet from one another so that IP packets are properly transmitted.

IP addresses appear in dotted decimal (rather than in binary) notation. Dotted decimal notation divides the 32-bit value into four 8-bit groups, or octets, and separates each octet with a period. For example, 199.217.132.1 is an IP address in dotted decimal notation.

To accommodate networks of different sizes, the IP address has three divisions – Classes A for large, B for medium and C for small. The difference among the network classes is the number of octets reserved for the network ID and the number of octets reserved for the host ID.

Class	Value of First Octet	Network ID	Host ID	Number of Hosts
A	1-126	First octet	Last three octets	16,387,064
B	128-191	First two octets	Last two octets	64,516
C	192-223	First tree octets	Last octet	254

Any value between 0 and 255 is valid as a host ID octet except for those values the InterNIC reserves for other purposes

Value	Purpose
0, 255	Subnet masking
127	Loopback testing and interprocess communication on local devices
224-254	IGMP multicast and other special protocols.

Subnetting and Subnet Masks
Subnetting divides a network address into sub-network addresses to accommodate more than one physical network on a logical network.

For example:
A Class B company has 100 LANs (Local Area Networks) with 100 to 200 nodes on each LAN. To classify the nodes by its LANs on one main network, this company segments the network address into 100 sub-network addresses. If the Class B network address is 150.1.x.x, the address can be segmented further from 150.1.1.x through 150.1.100.x

A subnet mask is a 32-bit value that distinguishes the network ID from the host ID for different sub-networks on the same logical network. Like IP addresses, subnet masks consist of four octets in dotted decimal notation. You can use subnet masks to route and filter the transmission of IP packets among your sub-networks. The value “255” is assigned to octets that belong to the network ID, and the value “0” is assigned to octets that belong to the host ID.

For the example above, if you want all the devices on the sub-networks to receive each other’s IP packets, set the subnet mask to 255.255.0.0. If you want the devices on a single sub-network only to receive IP packets from other devices on its own sub-network, set the subnet mask to 255.255.255.0 for the devices on the sub-network.

Subnet Mask	Routing and Filtering
0.0.0.0	IP packets are transmitted to all devices.
255.0.0.0	IP packets are only transmitted to devices that are IP that’s first octet matches the sender’s IP address’s first octet.
255.255.0.0	IP packets are only transmitted to devices that are IP that’s first two octets match the sender’s IP address’s first two octets.
255.255.255.0	IP packets are only transmitted to devices that are IP that’s first three octets match the sender’s IP address’s first three octets.

Appendix C: Glossary

The Glossary defines the terms used in this User Manual

Term	Definition
Ethernet	Local Area Network technology, originally developed by Xerox Corporation, can link up to 1,024 nodes in a bus network. Ethernet provides raw data transfer in a rate of 10 megabits/sec. with actual throughputs in 2 to 3 megabits/sec. using a baseband (single-channel) communication technique. Ethernet uses carrier sense multiple access collision detection (CSMA/CD) that prevents network failures when two devices attempt to access the network at the same time. LAN hardware manufacturers use Ethernet protocol; their products may not be compatible.
Gateway	A computer that attaches to a number of networks and routes packets between them. The packets can be different protocols at the higher levels.
IP	Internet Protocol – The TCP/IP standard protocol defines the IP datagram as the unit of information passed across a network.
IP Address	Internet Protocol Address – A 32-bit address assigned to hosts participating in a TCP/IP network. The IP address consists of network and host portions. It is assigned to an interconnection of a host to a physical network.
MAC	Medium Access Control - The network layer between the physical and the data link layers. Specifically, the physical (hardware) address exists in this layer.
MIB	Management Information Base – The database, i.e. set of variables maintained by a gateway running SNMP
NMS	Network Management Station
OID	Object Identifier – The variables defined in a MIB
Router	A computer that manages traffic between different network segments or different network topologies. It directs the destination IP address. The network media can be different, but the higher-level protocols must be the same.
SNMP	Simple Network Management Protocol – A standard protocol used to monitor IP hosts, networks, and gateways. SNMP defines a set of simple operations that can be performed on the OIDs of the MIBs managed by the monitored Agents. It employs the UDP/IP transport layer to move its object between the Agents and the NMS
TCP/IP	Transmission Control Protocol/ Internet Protocol – A protocol suite used by more than 15 million users with a UNIX association and widely used to link computers of different kinds.

Appendix D: Q&A

Q1. I forgot my password how can I retrieve it?

There are four different types of password for the iGuard system: ***Web Server Password***, ***Netility/Device Password***, ***iGuardView PC Application Password***, and the ***Master Password***

1. *Web Server Password*: the password you use to login from remote site. On V2.5 firmware the default login name is "admin" (lower case) and the password is the same as the master password which is printed on the serial label(All CAP). For V2.51 and later firmware, the default login and password is not defined. If you loose this password after you define it, you can use the master password to retrieve it (see below) or you can refresh the firmware if you know the device password. Download the firmware and use *iGuard Utility* to upload it into iGuard. Once completed, the Username and Passwords will be reset to default (blank).

2. *Netility/Device Password*: This is the password you use to setup iGuard via iGuard Utility program or when you want to refresh your firmware. By default this password is the same as Master Password which is located on the serial # label on the back of the iGuard. You can change this password under "IP Configuration/Advanced" in iGuard Utility. If you loose this password, you can use the master password to retrieve it (see below).

3.*iGuardView PC Application Password*: This is the software that you can install on a remote PC to monitor all iGuard cameras in multiple windows. You can use the admin account to setup multiple accounts so that users with different privilege level can use iGuardView to monitor the camera. By default the admin password is not defined. If you loose this password once defined, you will have to uninstall iGuardView and reinstall it.

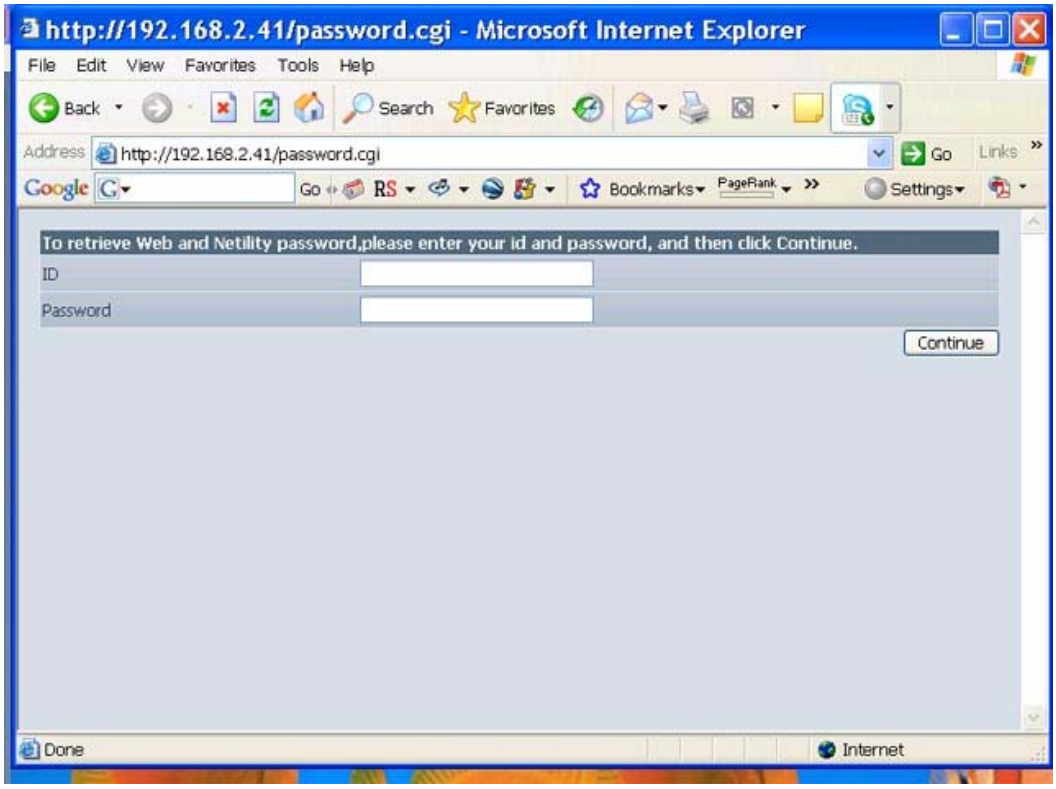
4.*Master Password*: This is the password that is printed on the serial label. You can use this password to retrieve your lost/forgotten Web Password and Netility/Device Passwords following the steps below:

In your browser please enter:

Http://xxx.xxx.xxx.xxx/password.cgi or Http://xxx.xxx.xxx.xxx:###/password.cgi

where xxx.xxx.xxx.xxx is the IP address of the iGuard, and ### is the port number that is assigned to the unit (by default it is 80)

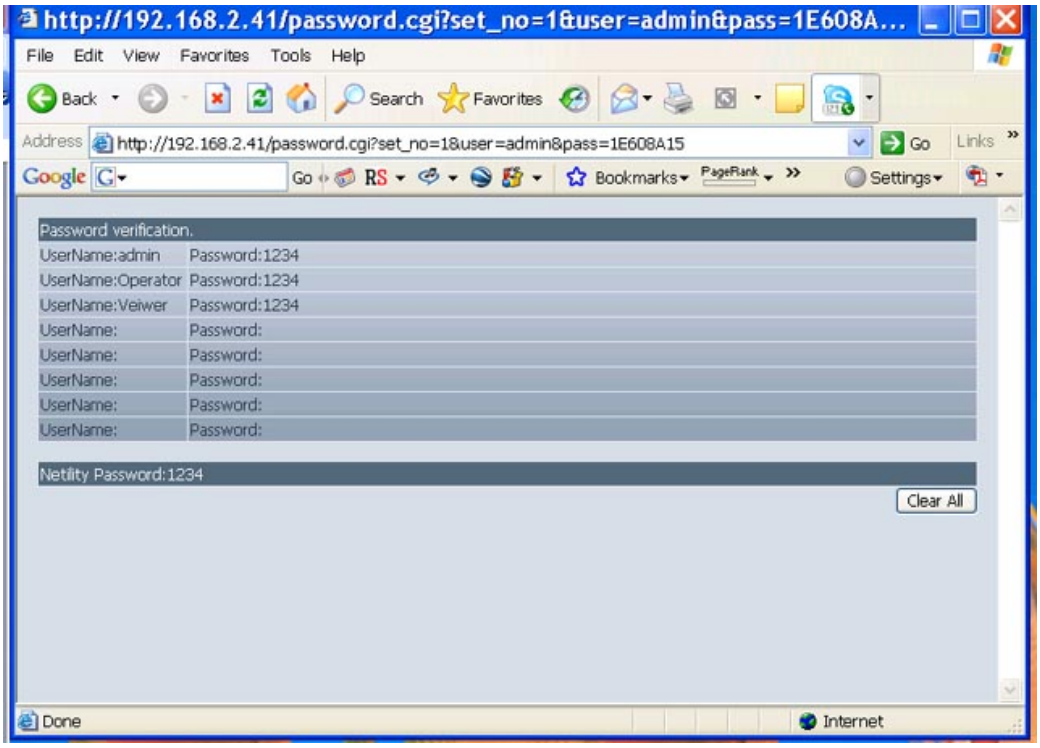
If the network is setup properly you will be prompted with a login-in screen:



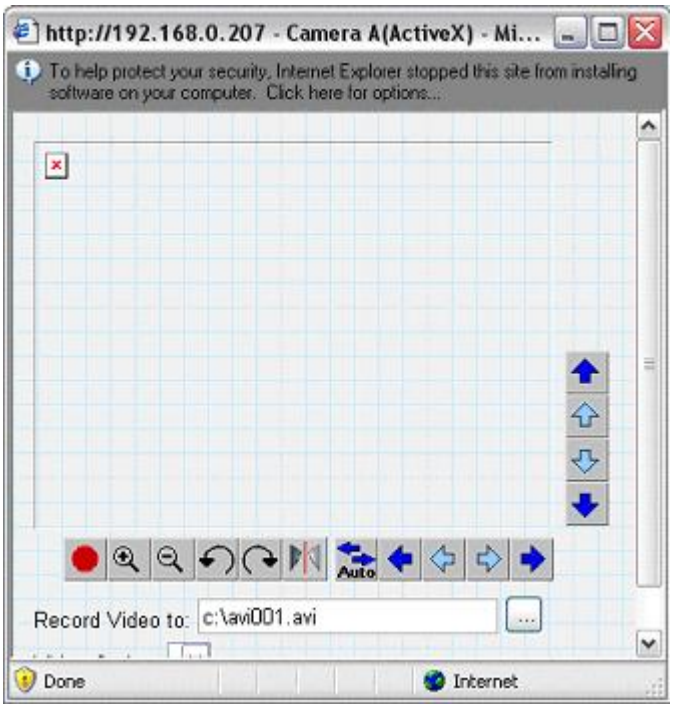
Your login ID is "admin" (lower case)

and the password is your "master password" (ALL CAP)

If the login is correct, the next screen will display all the Web and Netility/Device passwords that were assigned. You can click on the "Clear" button to reset all the passwords.



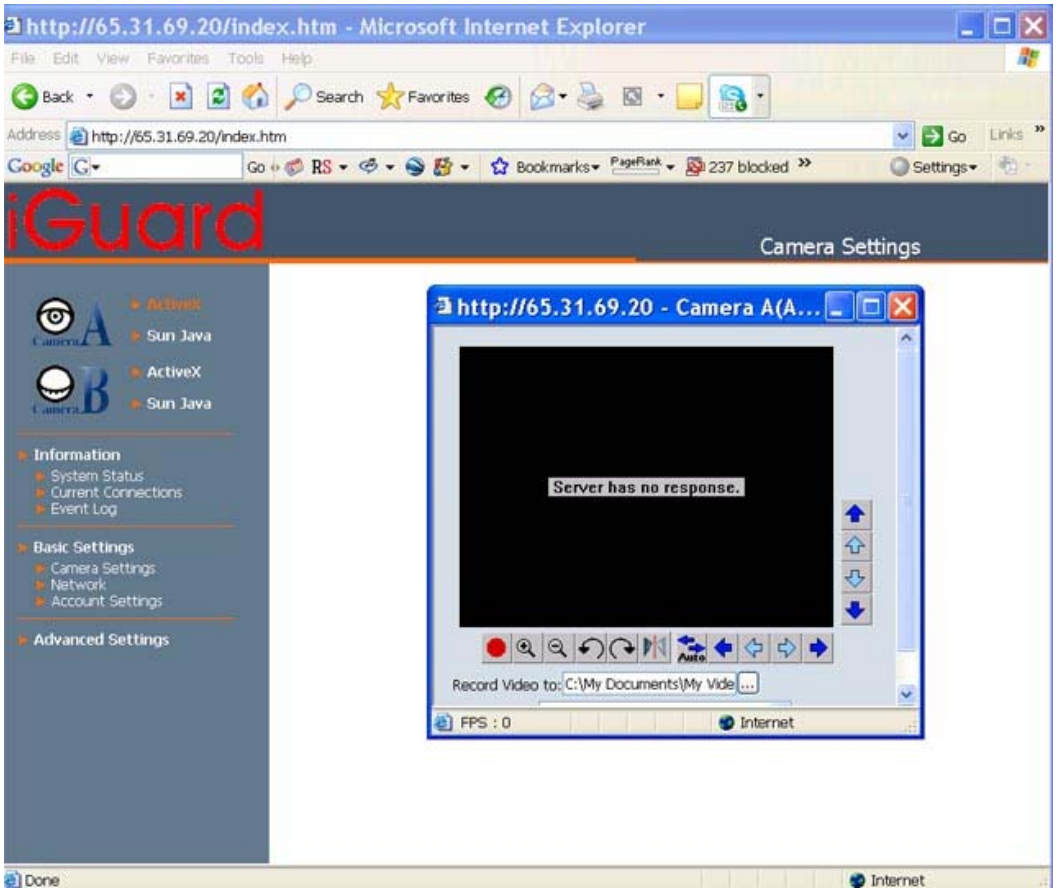
Q2. I get the following message, when I click on ActiveX button next to the camera A or B button



Click on the top margin, and install ActiveX. Confirm "yes" if prompted. Make sure you allow Active X components under Tools/Options/Security settings.

Note: Some third party web browser, such as Firefox, does not support ActiveX script, you will have to use Sun Java to view the camera.

Q3. I can connect to the camera, and ActiveX components are properly installed, but I still get the "Server has no response" Message



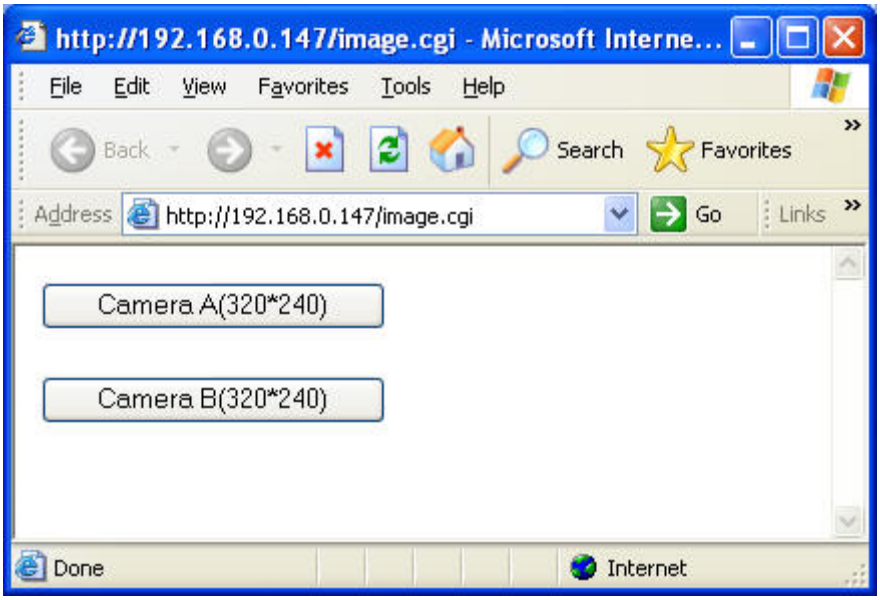
This is due to your firewall setting in your router or computer. iGuard uses UDP port 9001 by default to stream video from the camera. Your security setting has to allow traffic on this port.

Q4. Can I use other USB Camera to connect to iGuard?

Yes, provided that the camera is using VIMICRO chip. You will have to check with the manufacturer of the USB camera. Currently, about 60% to 70% of the cameras produced in China uses this chip.

Q5. How can I view images from my web enabled PDA?

Please make sure that you have a GRPS enabled PDA. Use the browser and type in **http://xxx.xxx.xxx.xxx/image.cgi** (where xxx is the WAN IP address or your Domain Name). You will then be directed to this page;



Click on either "Camera A (320*240)" or "Camera B (320*240)" to view the image.

Click "Refresh" to download the next image. Click "Back" to go back to the above page.

Q6. What is the effective length of the USB cable?

The industrial Standard for effective USB cable length is 5.0m from source to source. If you so decide to extend the length, you can purchase a USB extension

Q7. What is the effective length of the RJ-45 cable?

The Standard effective length per RJ-45 cable is 100m, you will need a hub per 100m extension, up to a maximum of 480m.

Q8. Can I use iGuard outdoors?

iGuard is designed primarily for indoor use. For outdoor use you will need a protective housing. This is not supplied.

Q9. Is the camera capable of zooming by adding a zoom lens?

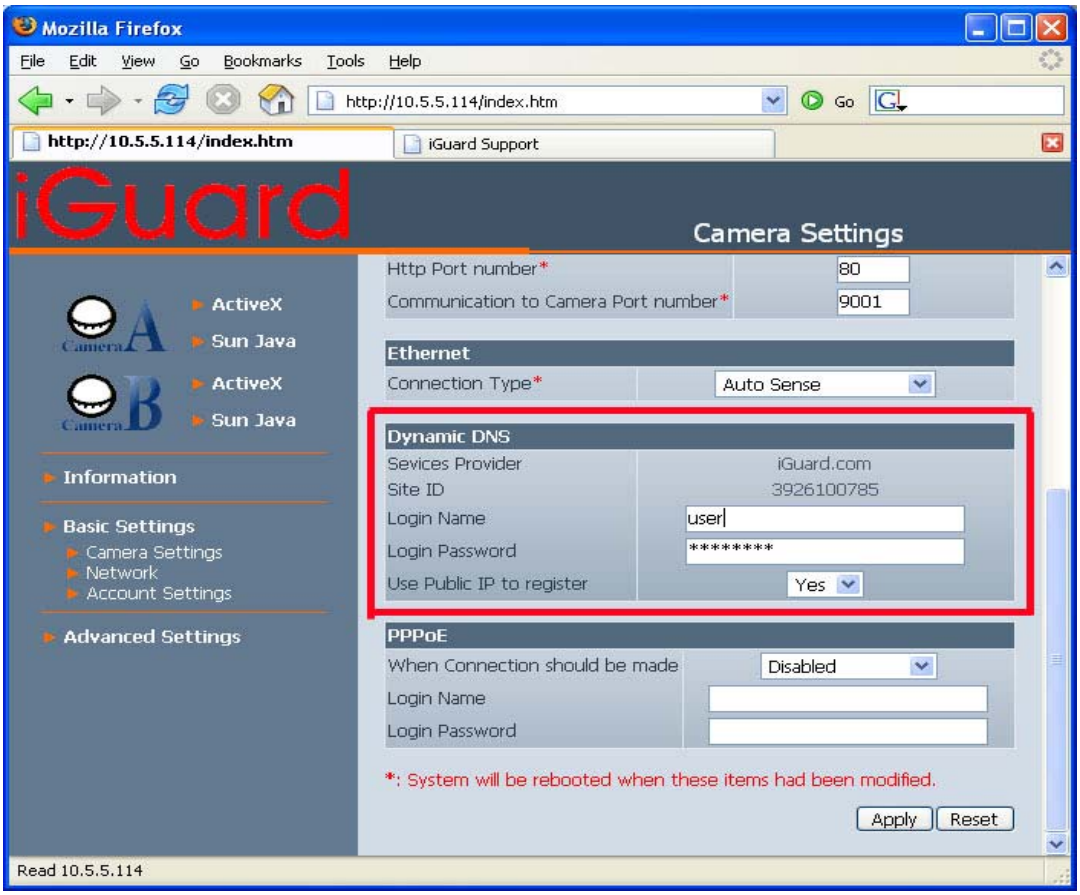
You can add a zoom lens, but will have to adjust the zoom manually. The default camera does not support 'remote' zoom.

Q10. My iGuard is connected to a Router and I can see it in LAN but my friends can't see it from the Web? How do I set up iGuard for the web?

For users with DYNAMIC IP;

(a) Contact iGuard.com Customer Support for a DDNS account (self-registration coming soon) and register your iGuard cameras

(b) From your PC log-on to your iGuard as Administrator. Enter your username and password for your iGuard.com account. Make sure the "Use Public IP to Register" is set to "Yes" Then Click "Apply" located at the bottom of screen.



Note: Please allow 5 minutes for the DDNS server to be updated with your Current WAN IP.

If iGuard is connected to a Router or IP Share then;

(d) Go to your Address Translation / NAT / Firewall section of your ROUTER. Open up TCP port 80 and UDP port 9001, make sure that the TCP port is not currently used by your router, otherwise choose a different port.

Note: Here you are using iGuard to check your current WAN IP and update the DDNS server. Alternatively, if your ROUTER supports DDNS, you can input the above details (b) in your ROUTER. In which case, your ROUTER will update the DDNS server with your current WAN IP.

If iGuardView is connected to your xDSL line or HUB, then;

(e) In iGuard, goto Basic Settings --> Network --> PPPoE, and enter the details.

For users with STATIC IP; proceed directly to (d) or (e).

Q11. I'm connecting iGuard to a HUB, how do I set it to access the internet?

1. Make sure that PPPoE section in iGuard is setup to connect to your ISP, and;

2. Make sure that Dynamic DNS in iGuard is setup.

Q12. I can not access iGuard Web Manager. I have opened up all the ports.

1. Check that your Router and iGuard are not both also using EXTERNAL / WAN port 80. If it is, change one to another EXTERNAL / WAN port.

2. If you changed iGuard default HTTP port 80 to another say, port 8081. Then you will have to redirect your web browser by typing **http://xxx.xxx.xxx.xxx:8081** where http://xxx.xxx.xxx.xxx is iGuard IP address.

Q13. I can access iGuard Web Manager but cannot view images when clicking ActiveX / Sun Java.

Make sure that you have a UDP port 9001 opened.

Q14. There is no Port Forwarding Section in my Router.

Different Routers have different setup for this section. In general, a more advanced router will allow you to forward *Internal / LAN* port to an *External / WAN* port. You can assign an internal port number to be forwarded to a different external port number.

However, there are also Routers which can not do this. Your internal port = external port, and you are only allowed to open a *range* of ports. Please check with your router's manufacturer on how to open the port for your router.

Q15. I setup the Email Server (SMTP) but I can't seem to receive any emails.

Make sure that your Internet Security Software / SPAM software does not block outgoing emails.

Q16. What bandwidth is required by iGuard?

The average "Bytes of Image per Frame" is between 4Kbytes - 9Kbytes. This size is determined according to color saturation of the image captured. Therefore, the "Frame per Second" (FPS) = "Data transmission rate" (in Bytes/s) divided by "Bytes of Image per Frame" (Bytes/frame)

You can check your current FPS setting in iGuard. Network --> Account Settings --> FPS (default is 10)

At 10 FPS, iGuard will need about 40Kbytes - 90Kbytes of bandwidth.

NOTE:

bps = bits per second (8 bits =1 Byte)

Most ADSL throughput speed varies, and is dependent on distance and environmental constraints. In most cases the actual throughput is only about 75%.

If you are using 56Kbps dial-up, your average speed should be around 4 Kbytes/sec - 6 Kbytes/sec

If you are using 512Kbps ADSL, your average speed should be around 40 Kbytes/sec - 50 Kbytes/sec If you are using T1 (1536Kbps) ADSL, your average speed should be 120 Kbytes/sec or higher.

If you are using 2M (2000Kbps) ADSL, your average speed should be 160 Kbytes/sec or higher.